

Firma Digitale

Software Aruba Sign

Sommario

1	Prerequisiti hardware e software	4
2	Utilizzo Aruba Sign e Firma Remota.....	4
2.1	Attivazione Account Firma Remota e installazione Aruba Sign	4
	Attivare un account di Firma Remota	4
	Installazione e avvio Software Aruba Sign.....	4
2.2	Configurazione parametri Firma Remota su Aruba Sign	5
3	Firma e verifica file Aruba Sign - Firma Remota.....	7
3.1	"Firma" uno o più file in formato .p7m - Firma Remota.....	10
3.2	Firmare un singolo file in formato ASiC-S - Firma Remota	13
3.3	"Firma" di più file in formato ASiC-E - Firma Remota.....	15
3.4	Apposizione "Firma Parallela" - Firma Remota.....	17
3.5	Apposizione "Controfirma" - Firma Remota.....	19
3.6	Apposizione Firma PDF - Grafica (Firma Remota).....	21
3.7	Apposizione Firma PDF - Invisibile (Firma Remota)	24
3.8	Apposizione di Marche Temporali - Firma Remota.....	26
	Apposizione di Marche Temporali con Aruba Sign e un Dispositivo di Firma Digitale	27
	Verifica Marche Temporali Residue	28
3.9	Verifica di File Firmati (Aruba Sign e Firma Remota)	29
3.10	Verifica di marca temporale in Formato TSR (Aruba Sign e Firma Remota)	33
3.11	Verifica di marca temporale in Formato TSD (Aruba Sign e Firma Remota)	35
3.12	Generare PIN OTP con Dispositivi di Firma Remota	38
	Generare una password OTP con OTP Display	38
	Generare una password OTP con OTP USB	38
	Generare una password OTP con OTP Mobile.....	39
4	Sincronizzazione Dispositivo Firma Remota.....	41
5	Configurazione Proxy http (Firma Remota).....	42
6	Installazione e avvio del Software – Firma Digitale.....	43
6.1	Installare i driver dei Lettori di Firma Digitale	43
6.2	Installare i driver Smart Card.....	44
6.3	Installare il software Aruba Sign	45
7	Firma e verifica file Aruba Sign - Firma Digitale.....	46
7.1	Caricamento documenti da firmare e/o cartelle su Aruba Sign.....	46
7.2	Firma uno o più file in formato .p7m - Firma Digitale.....	47
7.3	Firma un singolo file in formato ASiC-S - Firma Digitale.....	49
7.4	Firma di più file in formato ASiC-E - Firma Digitale	51
7.5	Apposizione Firma Parallela - Firma Digitale	53
7.6	Apposizione Controfirma - Firma Digitale	55
7.7	Apposizione Firma PDF – Grafica - Firma Digitale.....	57
7.8	Apposizione Firma PDF – Invisibile - Firma Digitale	59
7.9	Apposizione di Marche Temporali - Firma Digitale	61
7.10	Verifica di file firmati - Firma Digitale	64
7.11	Verifica di Marca Temporale in formato TSR - Firma Digitale	65
7.12	Verifica di Marca Temporale in formato TSD - Firma Digitale.....	68
8	Funzioni disponibili Home Page Aruba Sign.....	70

8.1	Gestione Carta Aruba Sign (PC) - modifica PIN e PUK	70
8.2	Cifra e Decifra un file Aruba Sign (PC)	72
8.3	Configurazione Proxy http Aruba Sign	75
9	Import Certificato su Mozilla Firefox Firma Digitale (PC).....	75
	Verifica corretta importazione Certificato Aruba sign su Google Chrome	77
	Verificare la corretta importazione del Certificato da "Strumenti" di Google Chrome:.....	78
	Verifica corretta importazione Certificato Aruba Sign su Mozilla Firefox	80
	Verificare la corretta importazione del Certificato da "Strumenti" di Mozilla Firefox:	81
	Import Certificato" con Aruba Sign (MAC)	82

1 Prerequisiti hardware e software

La postazione cui viene collegato il **software Aruba Sign** deve possedere i seguenti prerequisiti:

Software

Sistemi Operativi:

- Windows, dalla versione 7 e successive su sistemi a 64 bit
- osx 10.7.4 64 bit in poi
- Linux ubuntu 16.04 32/64bit in poi

Rete

Di seguito i parametri di rete che devono possedere le postazioni alle quali viene collegata Aruba Sign:

Disponibilità di connessione Internet senza presenza di Proxy

Possibilità di poter instaurare connessioni HTTP, HTTPS e LDAP

2 Utilizzo Aruba Sign e Firma Remota

2.1 Attivazione Account Firma Remota e installazione Aruba Sign

I **Kit di Firma Remota** sono composti da:

- **Certificato di Firma digitale che risiede presso un server sicuro di Aruba (HSM "Hardware Security Module")**;
- Dispositivo OTP (One Time Password);
- **Software di Firma e Verifica Aruba Sign**, che permettono al titolare di autenticarsi con le proprie credenziali e di firmare i propri file da qualsiasi postazione connessa a internet.

4

Attivare un account di Firma Remota

Per l'attivazione della Firma Remota con **Scratch Card** o **senza Scratch Card**, visionare la guida dedicata:

[Modalità di attivazione Firma Digitale Remota](#)

Installazione e avvio Software Aruba Sign

Una volta eseguita l'Attivazione del Kit di Firma Digitale Remota e la creazione del proprio Account, **installare il Software Aruba Sign**:

- 1) Collegarsi a <https://www.pec.it/download-software-driver.aspx>;
- 2) Dal menu a tendina "**Software**" → selezionare "**Software di Firma Aruba Sign**", quindi cliccare sul pulsante "**Scarica il Software**" corrispondente al sistema operativo utilizzato (l'esempio di seguito indicato si riferisce a Windows):

SOFTWARE


- Software di firma ArubaSign


Aruba Sign è il software che consente di apporre, gestire e verificare firme digitali e marche temporali. Dopo aver installato i driver della Card e/o del lettore, è necessario installare il software Aruba Sign sul tuo computer per la gestione del servizio di Firma.


N.B.: se disponi di «Aruba Key» non dovrai scaricare alcun software perché già installato nel tuo dispositivo.


Per installare Aruba Sign dovrai:


- Scaricare e salvare il file di installazione in base al sistema operativo presente sul tuo computer;
- Eseguire il file .exe;
- Completare la procedura di installazione.

Windows

[Scarica il Software](#)


Apple

[Scarica il Software](#)


Linux 64bit

[Scarica il Software](#)


Linux 32bit

[Scarica il Software](#)


Windows (ipovedenti)

[Scarica il Software](#)


Utilizzabile con:

Token


Smart Card


OTP display


OTP USB


OTP Mobile


+ Software per ArubaKey

+ Software rinnovo

1) **Scaricare ed eseguire su locale il File di installazione**, quindi installare il Software utilizzando la procedura guidata:

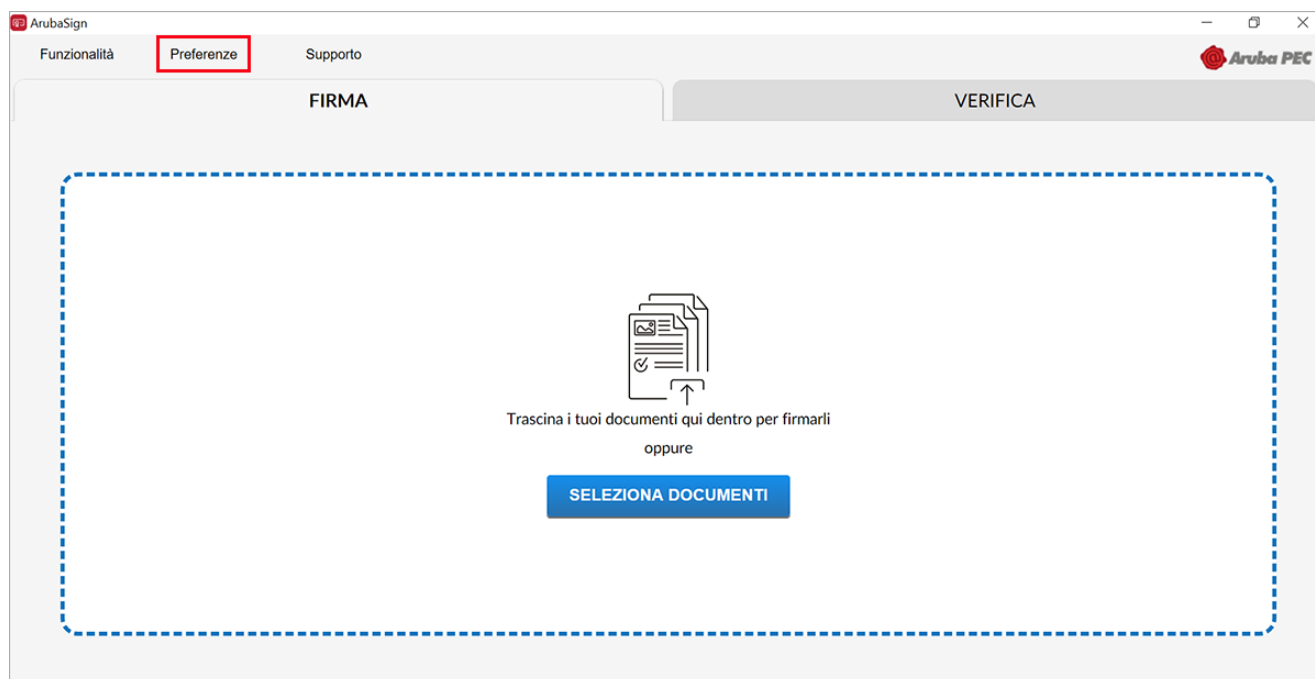
5

- Selezionare la **“Lingua di Installazione”**;
- Al Tab **“Installazione di Aruba Sign”**, cliccare su **“Avanti”**;
- Selezionare la **cartella di destinazione** e cliccare su **“Avanti”**;
- Premere **“Installa”** per continuare l'installazione;
- Attendere il completamento dell'installazione di Aruba Sign sul computer;
- Premere **“Fine”** per completare l'installazione.

2.2 Configurazione parametri Firma Remota su Aruba Sign

Una volta eseguita l'**attivazione della Firma Digitale Remota**, procedere all'installazione gratuita del Software di firma ArubaSign, è possibile la configurazione del proprio account (nome utente), per firmare documenti digitali, apporre marche temporali, e verificare i file firmati stessi. In caso di mancata configurazione è necessario inserire ad ogni utilizzo il nome utente e relativa password.

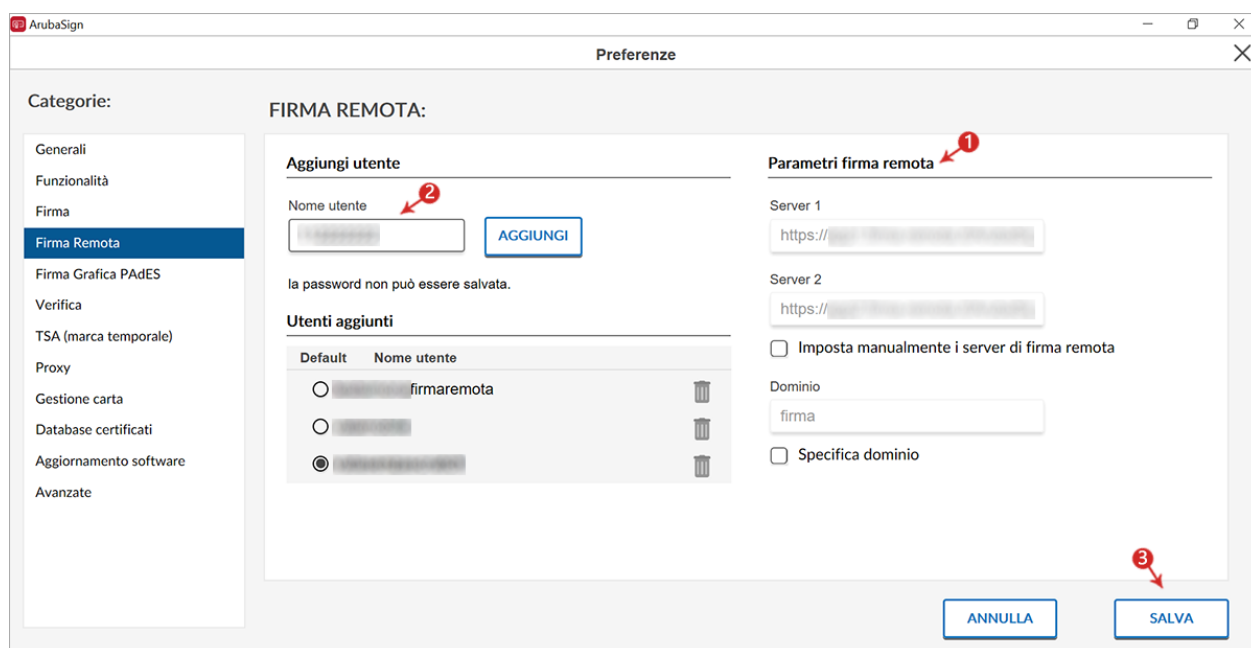
Per procedere, **avviare il software Aruba Sign**, quindi scegliere il menu **"Preferenze"**.



Selezionare **"Firma Remota"** e completare il Form come di seguito indicato:

- 1) In caso di soluzioni personalizzate, inserire manualmente i **parametri dell'indirizzo server primario e secondario**, inserendo il flag nella checkbox apposita o lasciare quelli **valorizzati automaticamente** dal sistema;
- 2) Scrivere il **"Nome Utente" Firma Remota** creato in fase di attivazione del servizio. Nel caso in cui il dominio sia "firma", cioè per soluzioni non personalizzate, è sufficiente inserire solo il nome utente, omettendo la specifica dominio;
- 3) Cliccare su **"Salva"** per completare l'operazione:

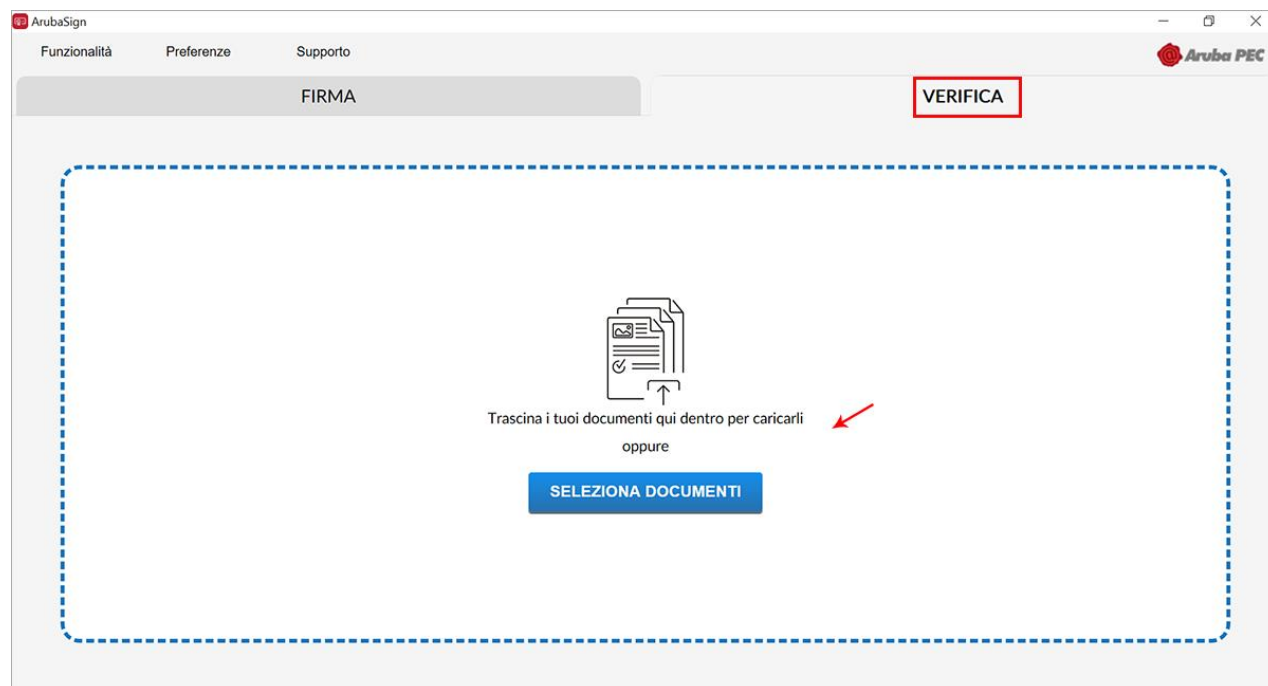
6



3 Firma e verifica file Aruba Sign - Firma Remota

La **Verifica dei File firmati** permette di verificare la **validità legale del certificato**.

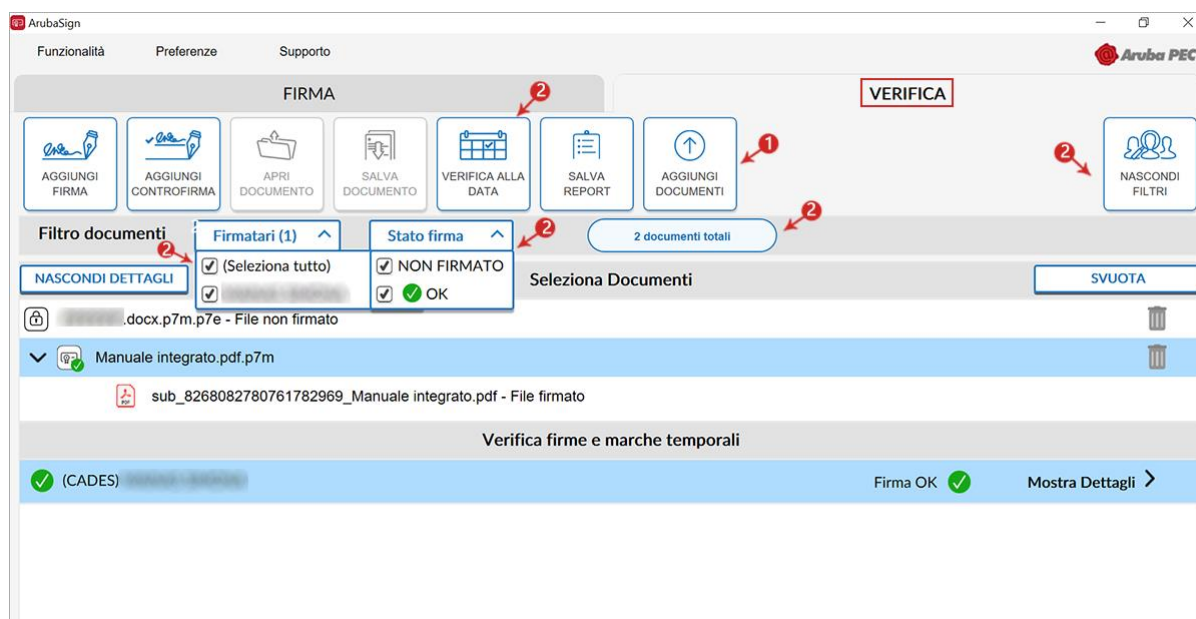
Per verificare uno o più file firmati con Aruba Sign, selezionare il documento nella scheda **"VERIFICA"**.



7

Alla schermata visualizzata è possibile:

- 1) Verificare ulteriori file firmati trascinandoli da locale o su **"AGGIUNGI DOCUMENTO"**;
- 2) Da **"Mostra/Nascondi Filtri"** sono riportati il nome e cognome del/i firmatario/i, il numero di firme che ha apposto, la data dell'ultima apposizione e lo "Stato" (esito) della verifica. Per visionare quali sono i documenti firmati da uno specifico firmatario, inserire il flag in corrispondenza del soggetto interessato, il nome appare a fianco dei singoli file che ha firmato presenti nell'area "Seleziona documenti":



3) "Verifica firme e marche temporali" sono visibili le firme presenti all'interno del file:

- **Firma valida**

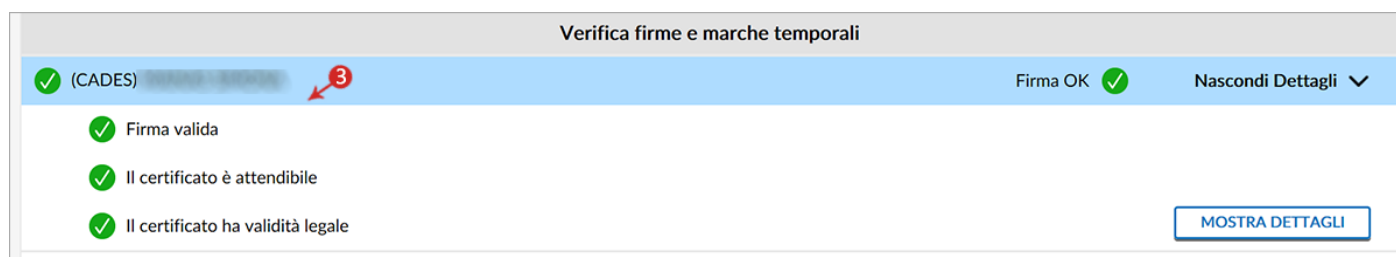
Attesta il formato della firma e che il documento non è stato alterato dopo la firma;

- **Il certificato è attendibile**

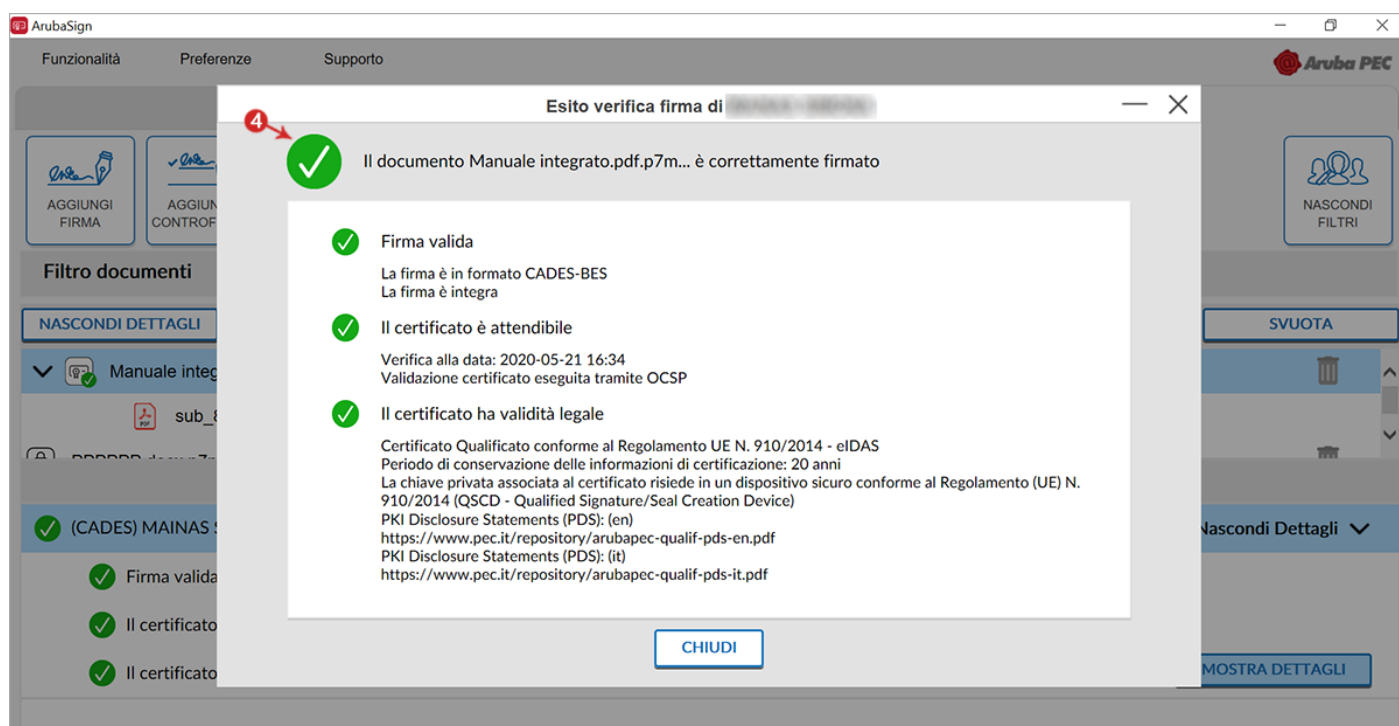
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della Verifica;

- **Il certificato ha validità legale**

Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



Da **Mostra Dettagli** è possibile verificare la validità della firma apposta:



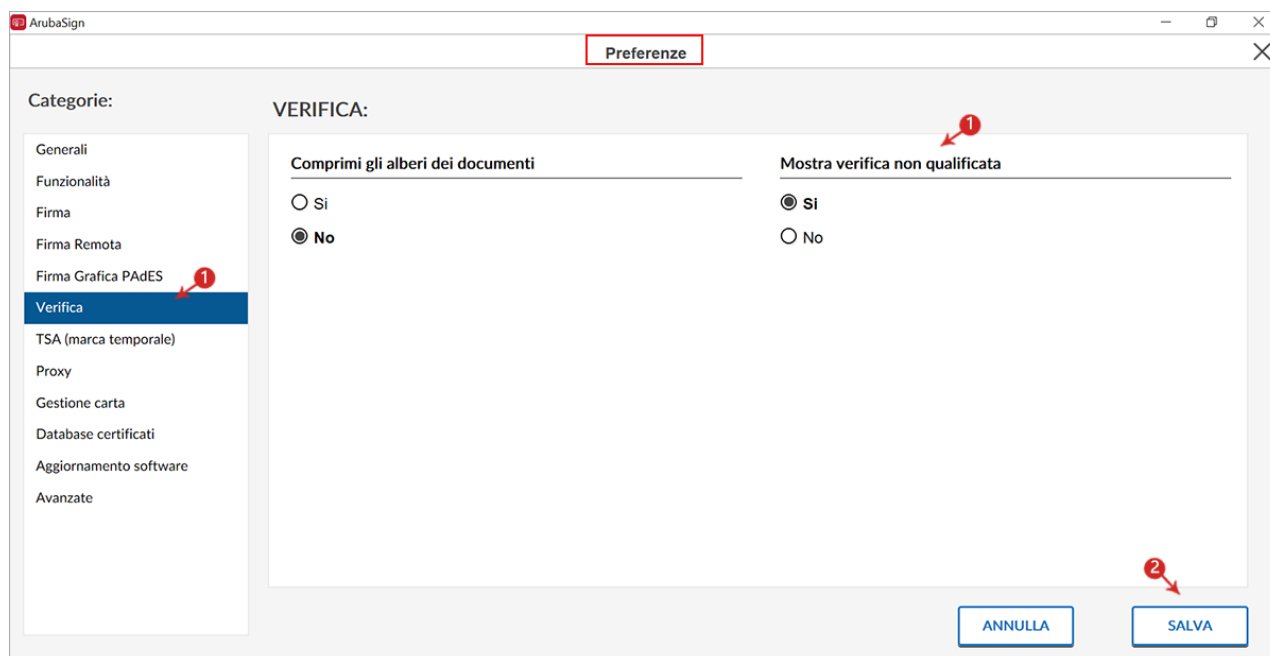
8

In caso di necessità è possibile attivare un'opzione che consente di verificare uno o più File Firmati con certificati non emessi da una Certification Authority. La verifica della Firma opposta può essere:

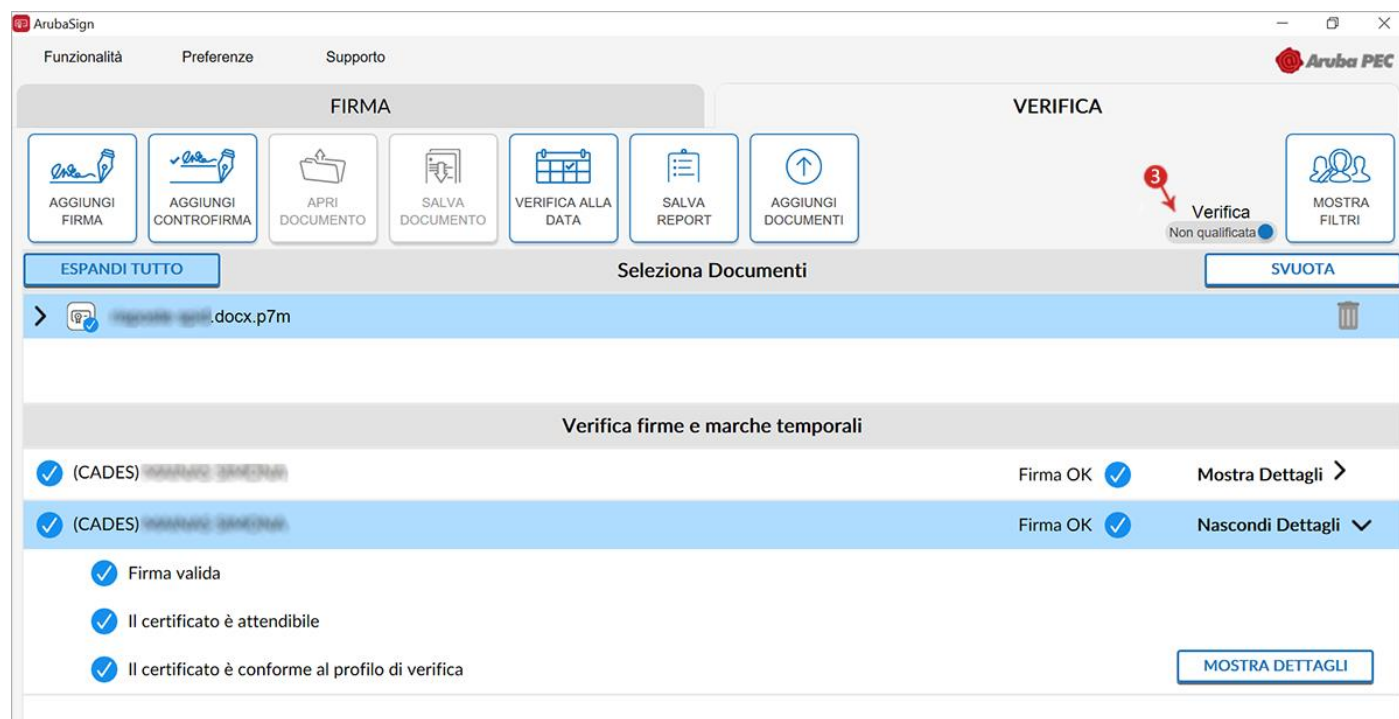
- **Non qualificata:** la firma è considerata valida se è integra e il certificato valido. Non è richiesto che sia emesso da una Certification authority di firma digitale.
- **Qualificata:** la firma apposta a un file è considerata valida se è integra, il certificato valido e rilasciato da una Certification Authority qualificata nel rispetto della normativa vigente circa la firma digitale qualificata.

Per attivare l'opzione, accedere su **Preferenze** di Aruba Sign:

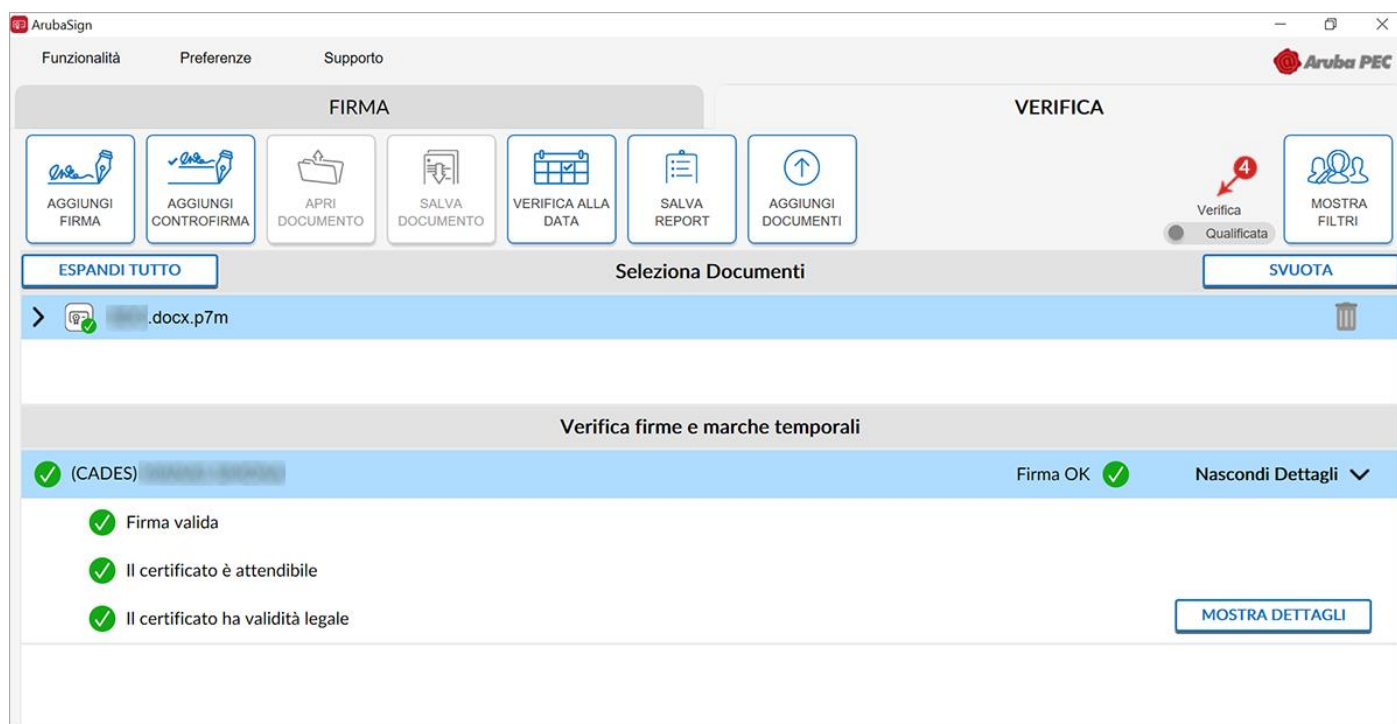
- 1) Su VERIFICA abilitare Mostra verifica non qualificata;
- 2) Confermare su **SALVA**:



L'opzione di verifica "**Non qualificata**" è attiva:



Se l'opzione non viene attivata, la verifica è **"Qualificata"**:



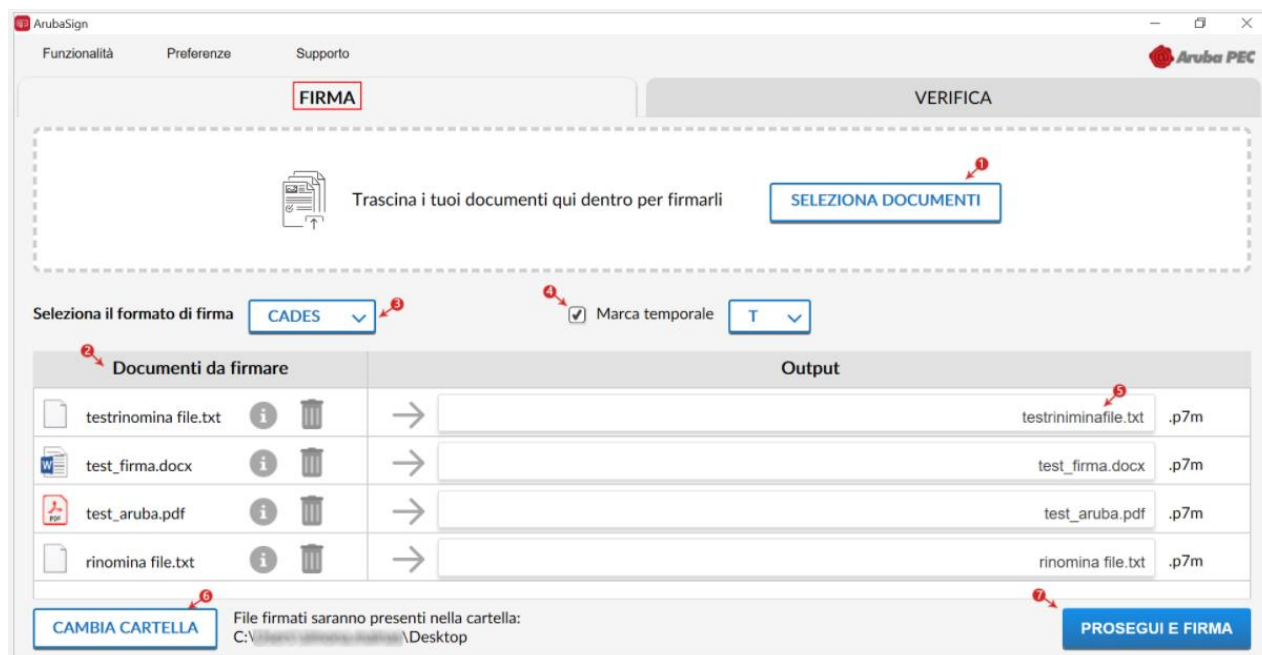
3.1 "Firma" uno o più file in formato .p7m - Firma Remota

Un file firmato digitalmente assume estensione **.p7m**, che si somma all'estensione del file originario. Ad esempio, un documento **.txt**, al termine del processo di Firma Digitale diviene un documento **.txt.p7m** che rappresenta una **busta informatica (PKCS#7)**. La busta incorpora al suo interno il documento originario, il certificato del sottoscrittore e un hash del documento firmato con il certificato del sottoscrittore. Un documento sottoscritto digitalmente ha piena validità legale.

Per firmare digitalmente uno o più file in formato **.p7m** (Firma CADES) e/o una intera cartella con Aruba Sign e Firma Digitale Remota:

- 1) Trascinare o selezionare uno o più documenti e/o una intera cartella;
- 2) Il singolo/i documenti caricati/o sono visibili all'apposita schermata **"Documenti da firmare"**;
- 3) Dall'apposito menu a tendina **"Seleziona il formato firma"** selezionare come tipologia di Firma **"CADES"** per firmare il file in formato **.p7m**;
- 4) Se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **"Marca Temporale"** nel formato scelto dall'apposito menu a tendina;
- 5) Dalla finestra **"Output"** rinominare, se desiderato, eventuali file prima di apporre la firma;
- 6) Da **"CAMBIA CARTELLA"** verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;

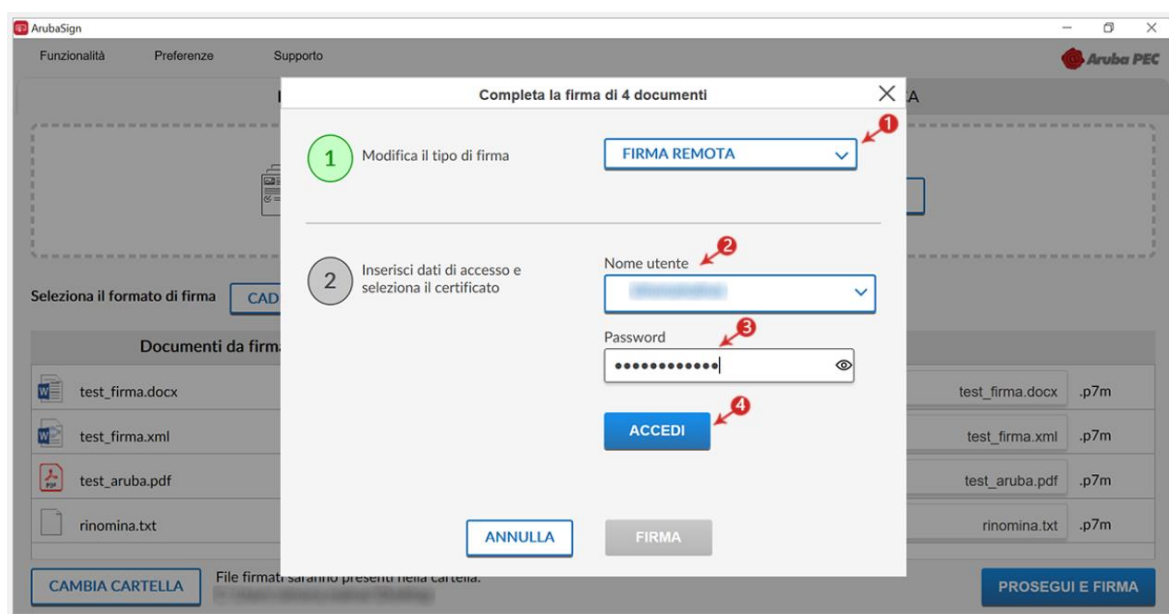
- 7) Cliccare su "**PROSEGUI E FIRMA**" per continuare. Sono firmati tutti i documenti presenti alla finestra "**Documenti da firmare**":



Alla schermata "Completa la firma di 4 documenti":

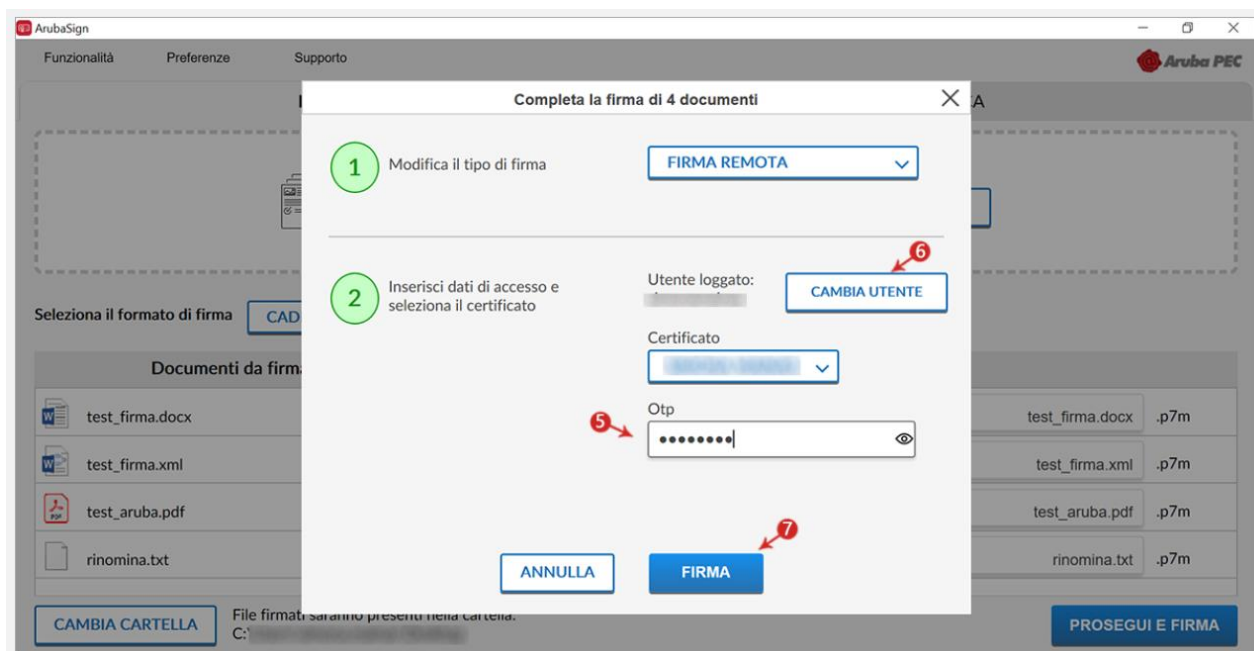
- 1) selezionare o modificare il **tipo di firma**;
- 2) inserire i dati di accesso "**Nome e utente**" del proprio account di Firma Digitale Remota;
- 3) inserire la "**Password**" del proprio account di Firma Digitale Remota;
- 4) cliccare su "**ACCEDI**" e proseguire:

11



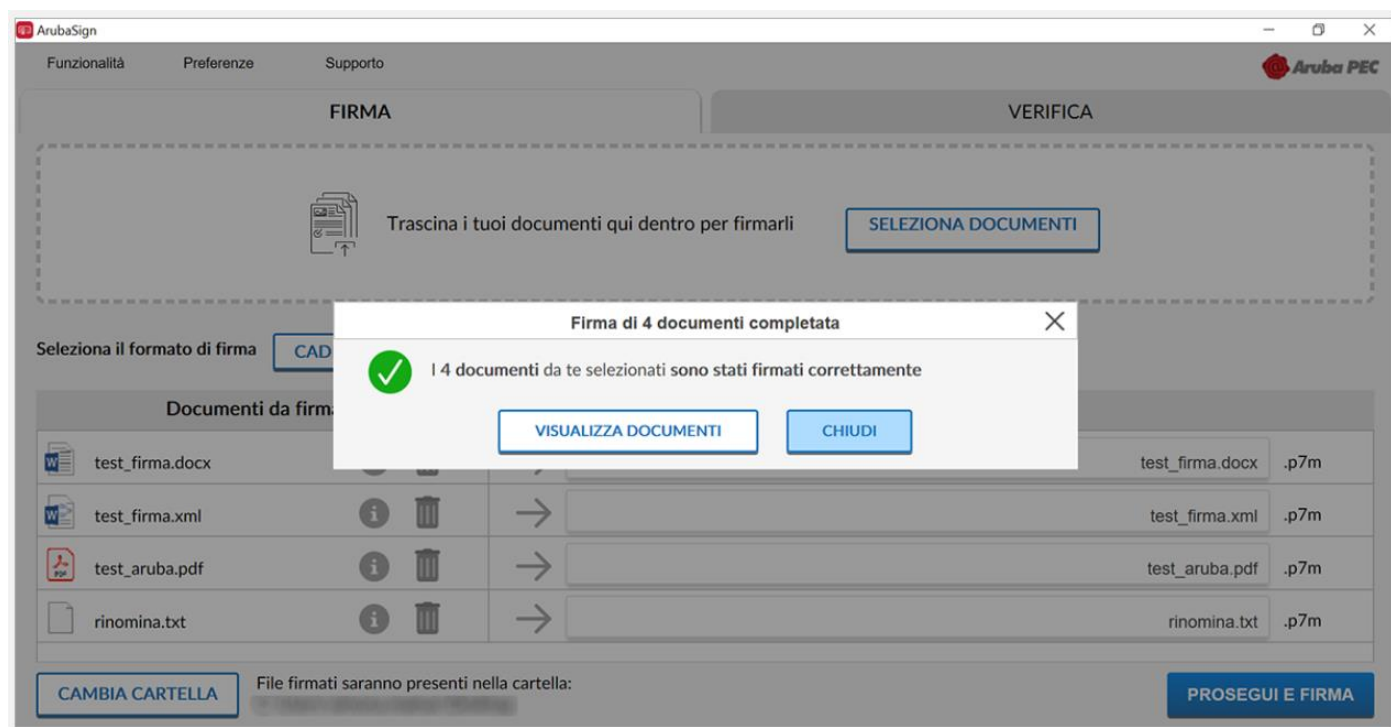
- 5) inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;

- 6) cliccando su "**CAMBIA UTENTE**" è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
- 7) Cliccare su "**FIRMA**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**CHIUDI**" per concludere:

12



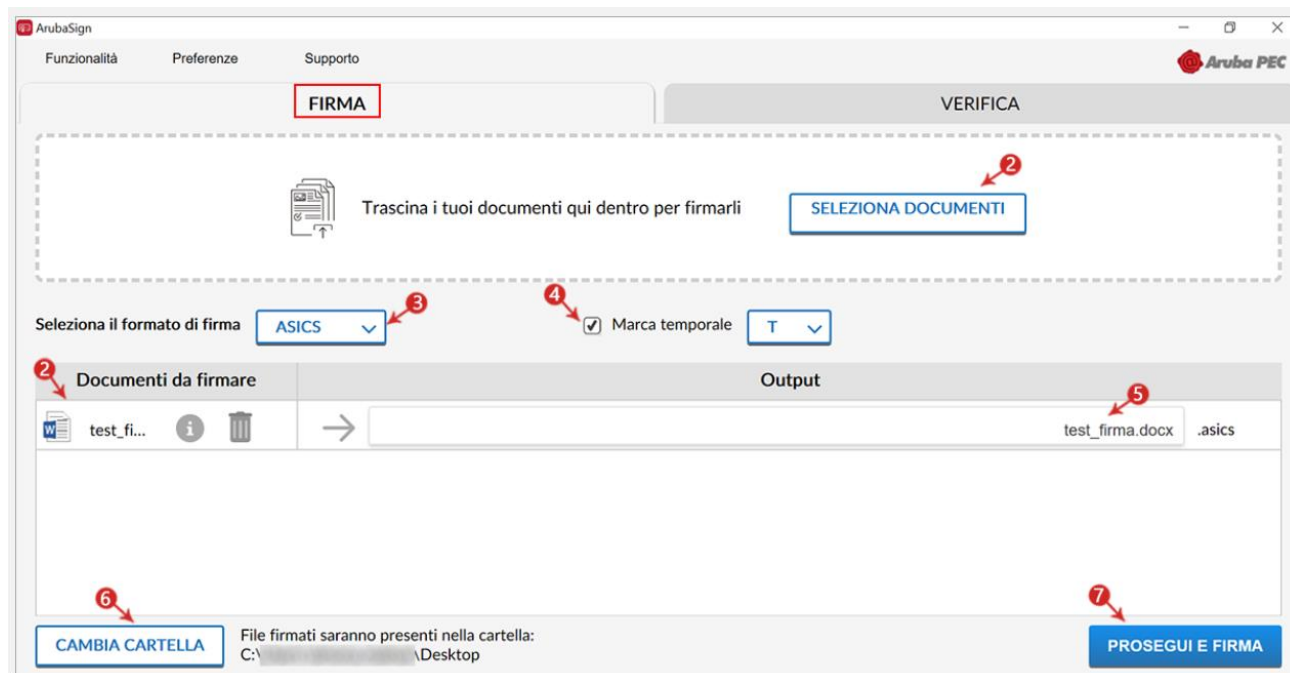
Il documento/i firmato/i sono salvati in formato .p7m nella cartella indicata in fase di Firma.

3.2 Firmare un singolo file in formato ASiC-S - Firma Remota

Il formato di firma **asic-s** (**A**ssociated **S**ignature **C**ontainers "**ASiC** simple") è un contenitore di dati che raggruppa un file e le relative firme digitali detached e/o marche temporali associate, utilizzando il formato .zip.

Per firmare digitalmente un file in formato ASiC-S con Aruba Sign e Firma Digitale Remota:

- 1) **Caricare il documento;**
- 2) Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di un singolo File, per firmare più file in formato ASiC, selezionare la specifica voce ASiC-E.
- 3) Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
- 4) Dall'apposito menu a tendina "**Seleziona il formato firma**" selezionare come tipologia di Firma "**ASiC-S**";
- 5) Se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce "**Marca temporale**" nel formato scelto dall'apposito menu a tendina;
- 6) Dalla finestra "Output" rinominare, se desiderato, il file;
- 7) Da "CAMBIA CARTELLA" verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
- 8) Cliccare su "**PROSEGUI E FIRMA**" per continuare:

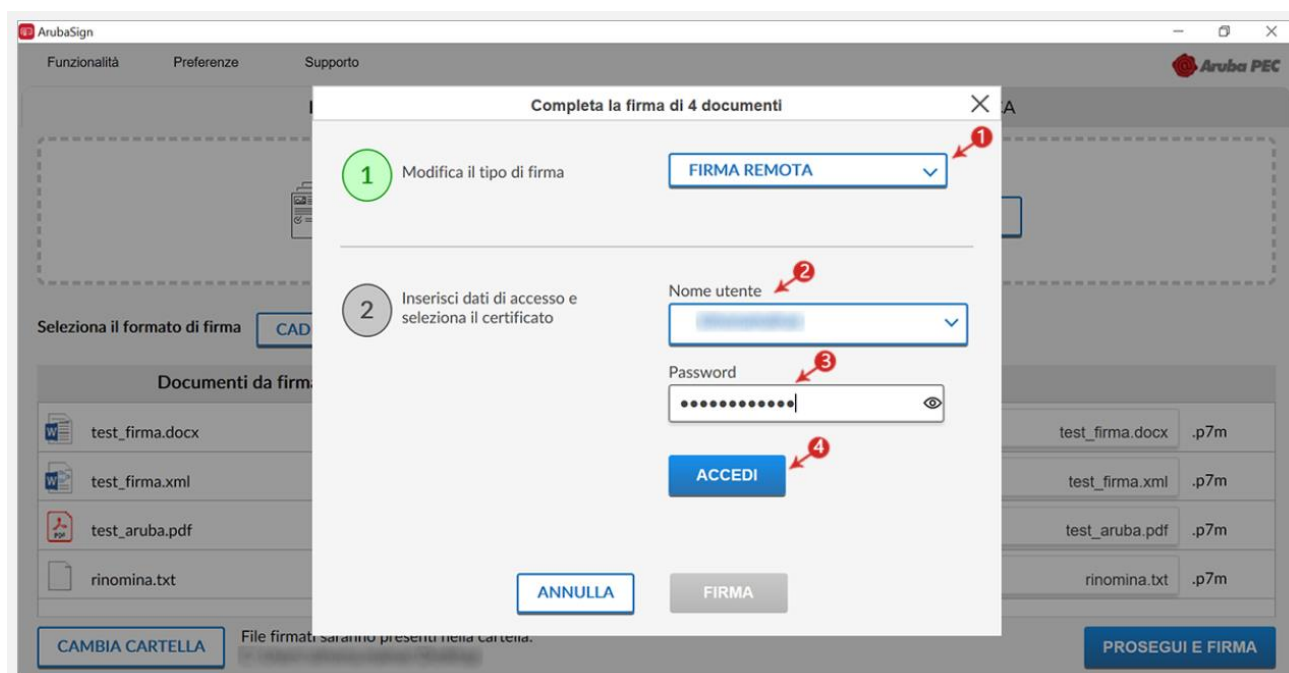


13

Alla schermata "Completa la firma di 4 documenti":

- 1) selezionare o modificare il **tipo di firma**;
- 2) inserire i dati di accesso "**Nome e utente**" del proprio account di Firma Digitale Remota;
- 3) inserire la "**Password**" del proprio account di Firma Digitale Remota;

4) cliccare su "**ACCEDI**" e proseguire:

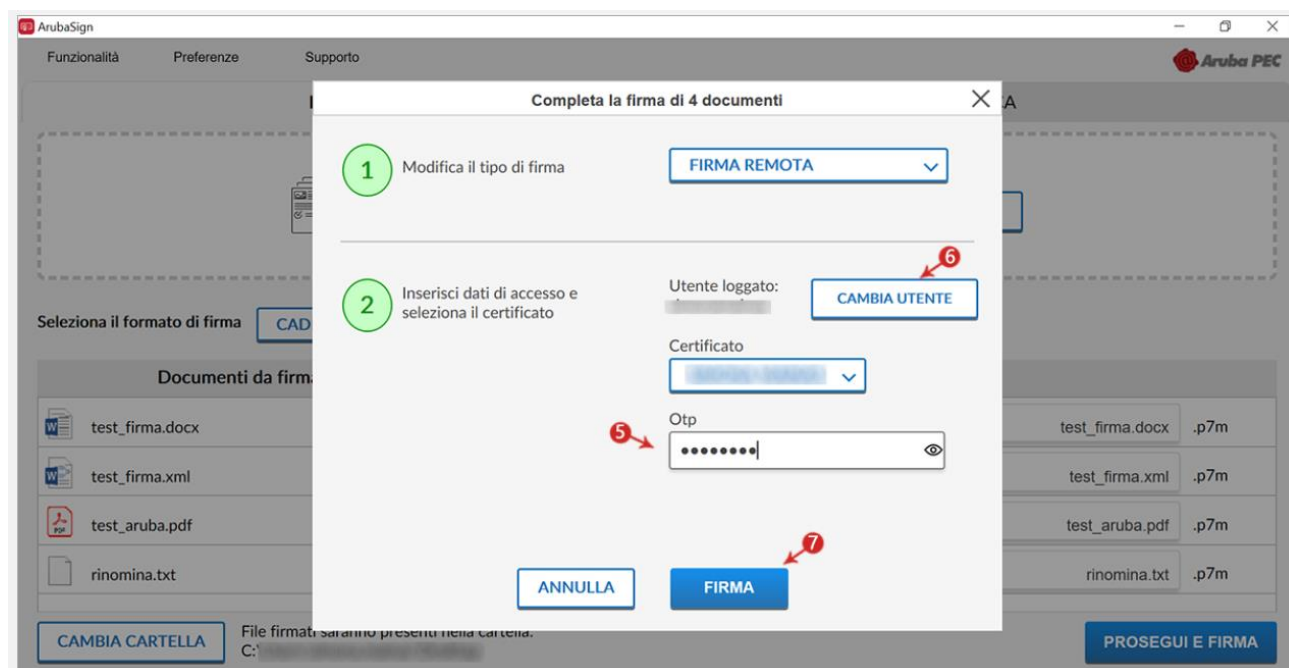


5) inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;

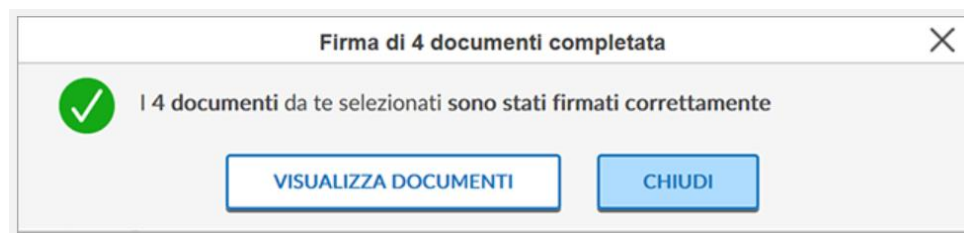
6) cliccando su "**CAMBIA UTENTE**" è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;

7) Cliccare su "**FIRMA**" per concludere il processo:

14



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su **"CHIUDI"** per concludere:



Il documento firmato in **formato ASiC-S** è salvato nella cartella indicata in fase di Firma.

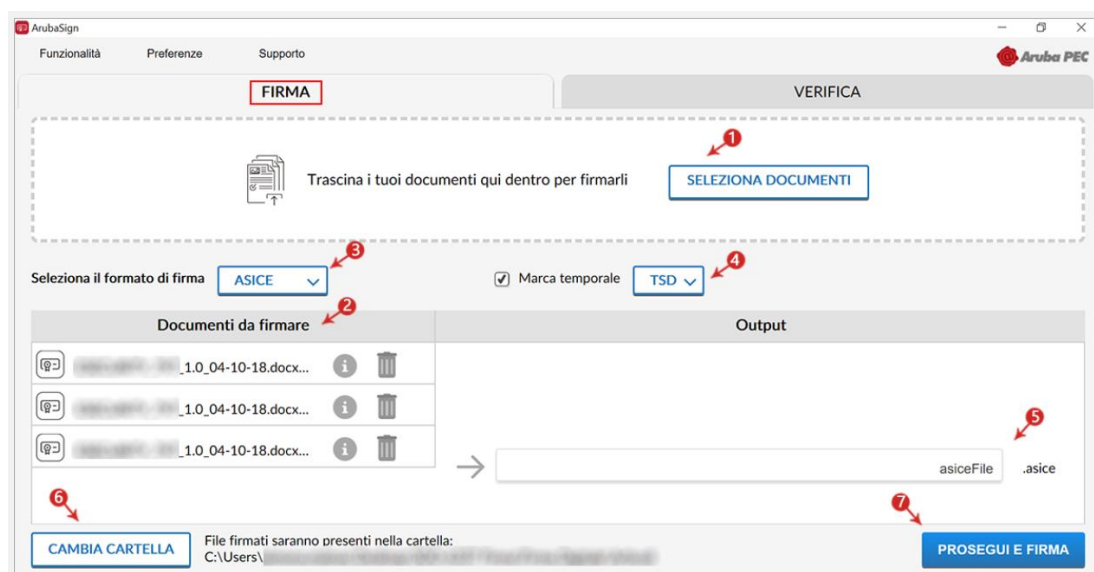
3.3 "Firma" di più file in formato ASiC-E - Firma Remota

Il formato di firma ASiC-E (**Associated Signature Containers "ASiC simple"**) è un **contenitore di dati che raggruppa più file e le relative firme digitali detached e/o marche temporali associate**, utilizzando il formato .zip.

Per **firmare digitalmente più file in formato ASiC-E con Aruba Sign e Firma Digitale Remota**:

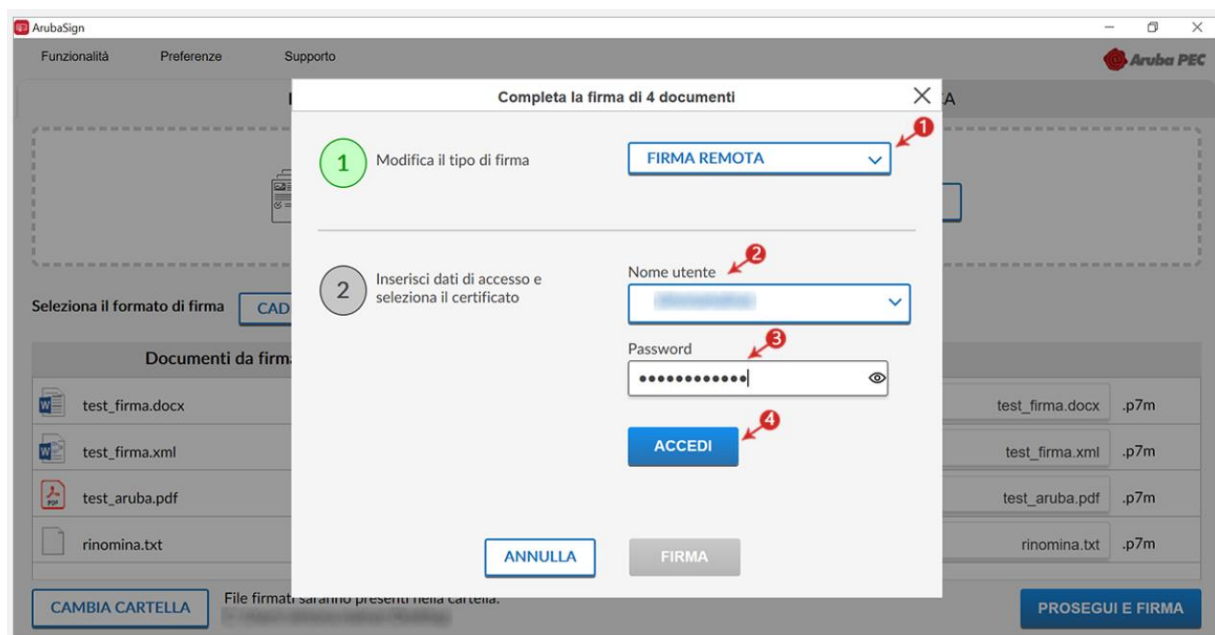
- 1) **Caricare i documenti e/o una intera cartella**;
Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di più documenti, per firmare un solo file in formato ASiC, selezionare dall'apposito menu a tendina **"Formato Firma"** ASiC-S.
- 2) I **documenti caricati** sono visibili all'apposita schermata **"Documenti da firmare"**;
- 3) Dall'apposito menu a tendina **"Seleziona il formato firma"** selezionare come tipologia di Firma **"ASiC-E"**;
- 4) Se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **"Marca temporale"** nel formato scelto dall'apposito menu a tendina;
- 5) Dalla finestra **"Output"** rinominare, se desiderato, il contenitore dei file;
- 6) Da **"CAMBIA CARTELLA"** verificare che il percorso utilizzato per salvare i file firmati sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
- 7) Cliccare su **"PROSEGUI E FIRMA"** per continuare. Sono firmati tutti i documenti presenti alla finestra **"Documenti da firmare"**:

15



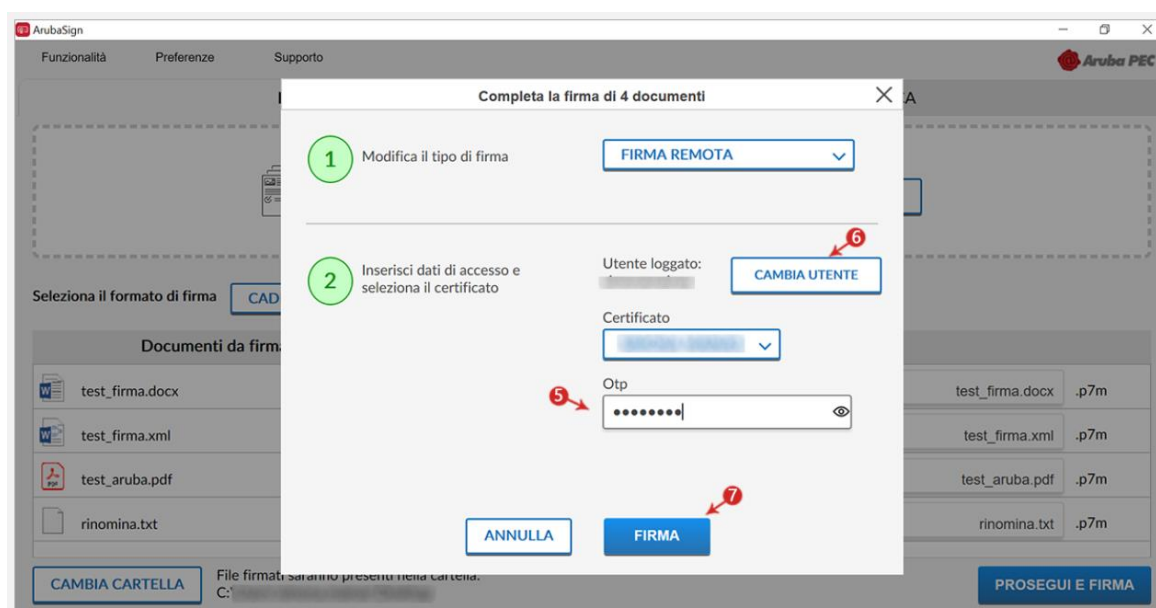
Alla schermata "**Completa la firma documenti**":

- 1) selezionare o modificare il **tipo di firma**;
- 2) inserire i dati di accesso "**Nome e utente**" del proprio account di Firma Digitale Remota;
- 3) inserire la "**Password**" del proprio account di Firma Digitale Remota;
- 4) cliccare su "**ACCEDI**" e proseguire:

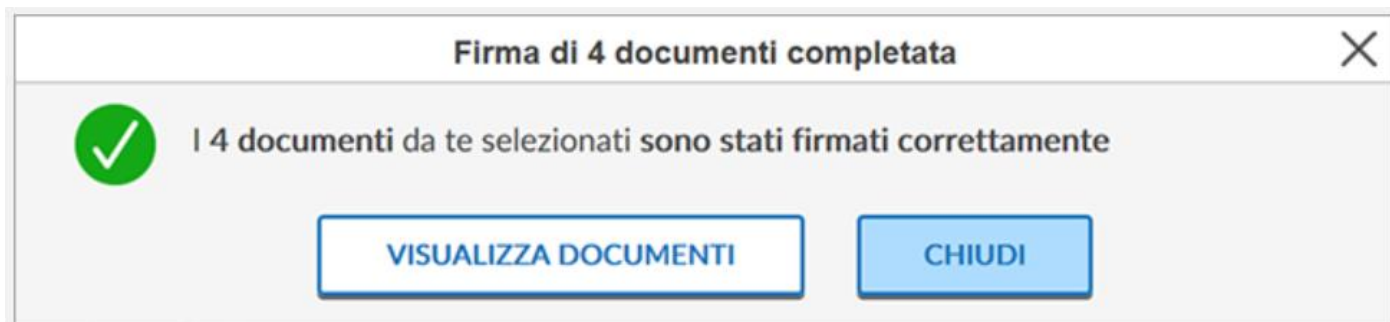


16

- 5) inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;
- 6) cliccando su "**CAMBIA UTENTE**" è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
- 7) Cliccare su "**FIRMA**" per concludere il processo:



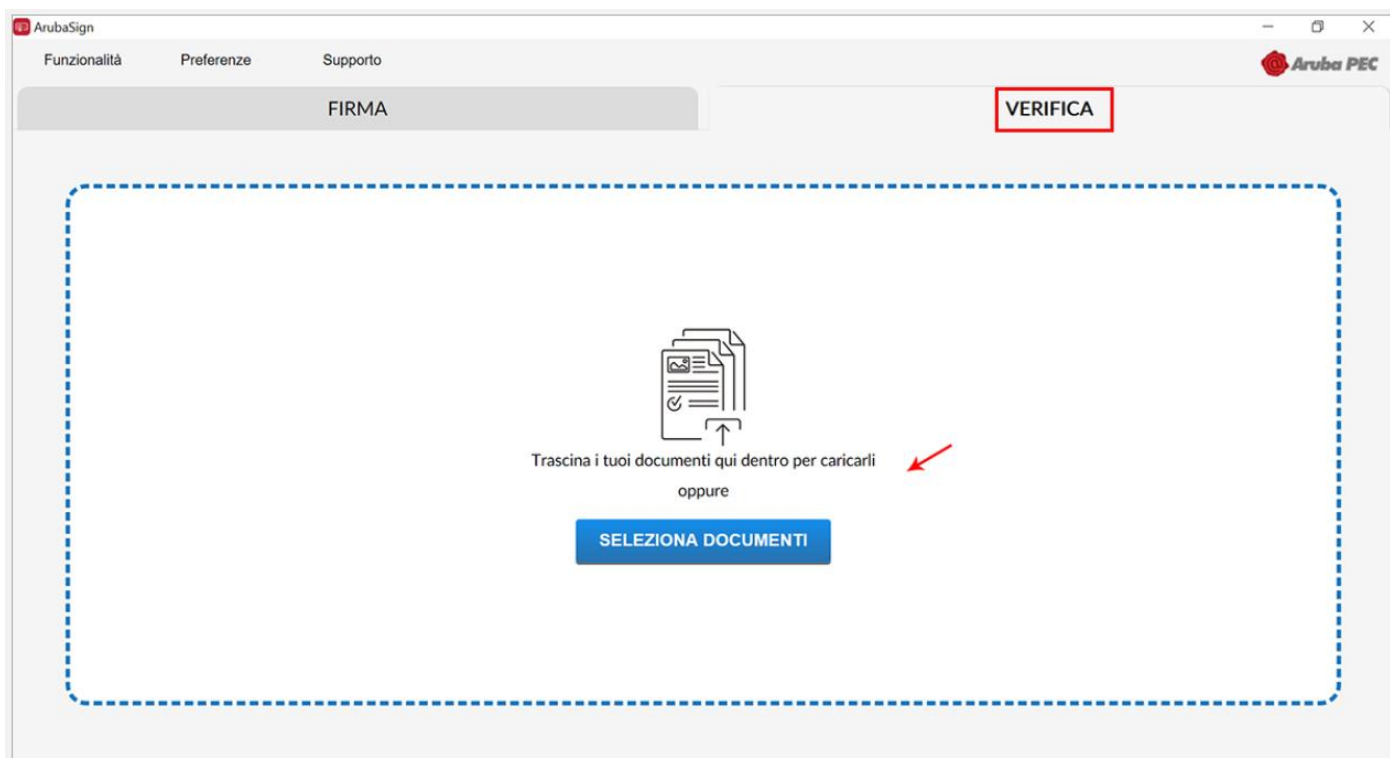
Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma dei file. Cliccare su "**CHIUDI**" per concludere:



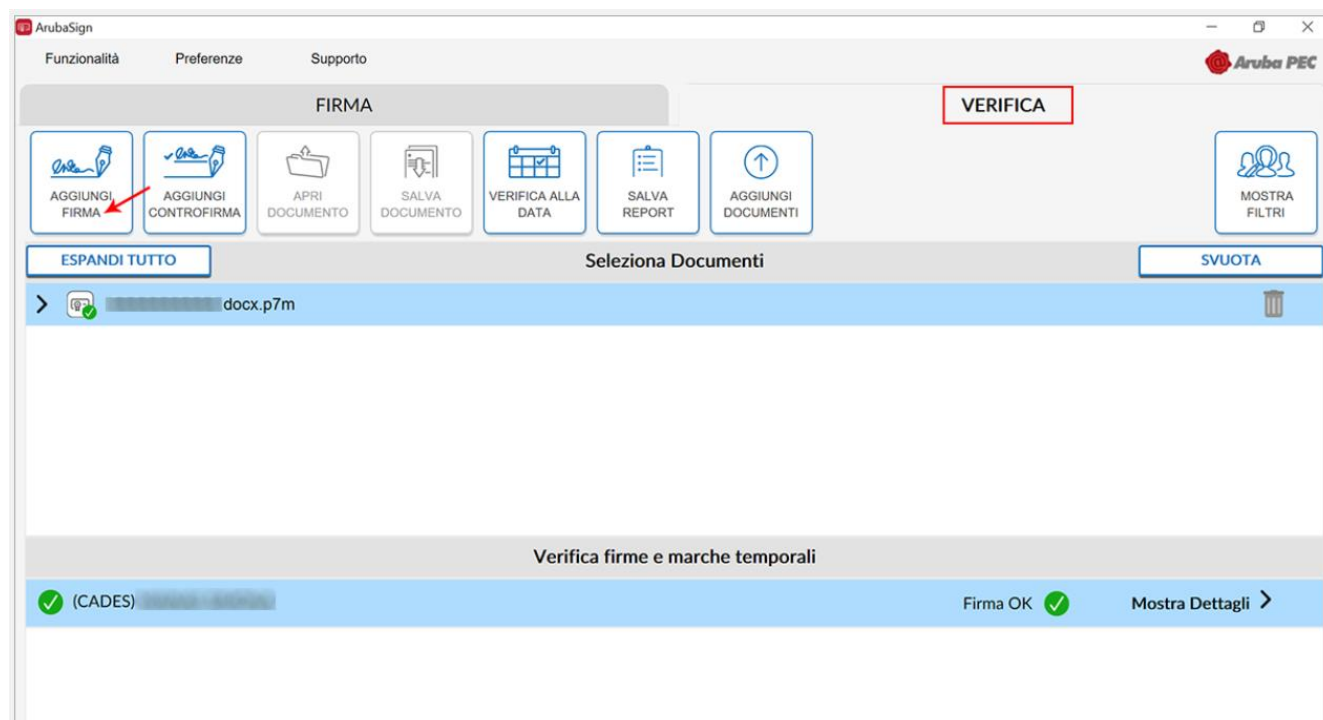
Il contenitore di documenti in **formato ASiC-E** è salvato nella cartella indicata in fase di Firma. In fase di verifica del contenitore è possibile visionare il dettaglio delle Firme apposte a ogni singolo documento.

3.4 Apposizione "Firma Parallela" - Firma Remota

La funzione "**Firma Parallela**" è accessibile trascinando o selezionando il documento all'interno della scheda **VERIFICA** del Software Aruba Sign **uno o più file già firmati in formato .p7m (CADES) o .PDF (PADES)**. È aggiunta allo stesso livello e allo stesso contenuto di una firma preesistente e viene di norma utilizzata per aggiungere firme ad un documento già firmato in formato .p7m in quei flussi documentali che ne prevedono l'utilizzo. Per crearla selezionare o trascinare **un file .p7m (CADES) o .PDF (PADES)**, su "**VERIFICA**" di Aruba Sign:



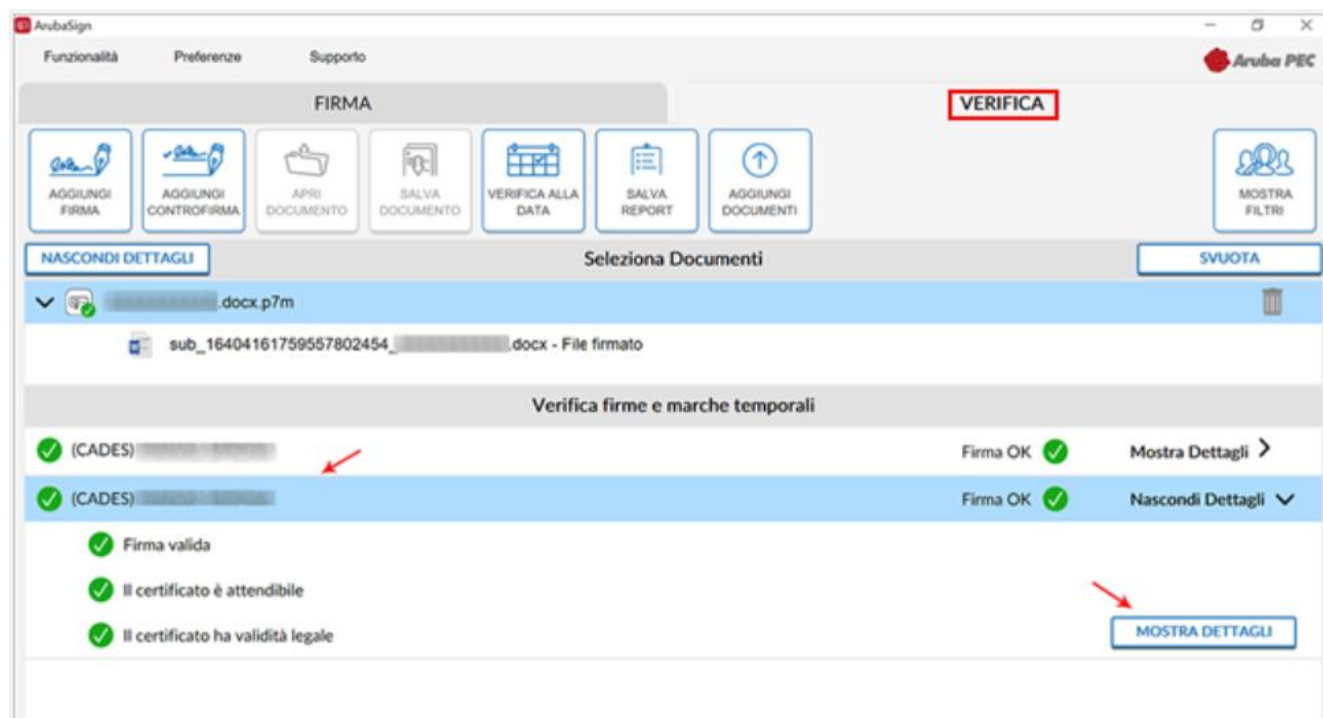
Selezionato il documento (anche in caso di caricamento di un solo file) su cui apporre la **Firma Parallela** poi cliccare su **"AGGIUNGI FIRMA"**:



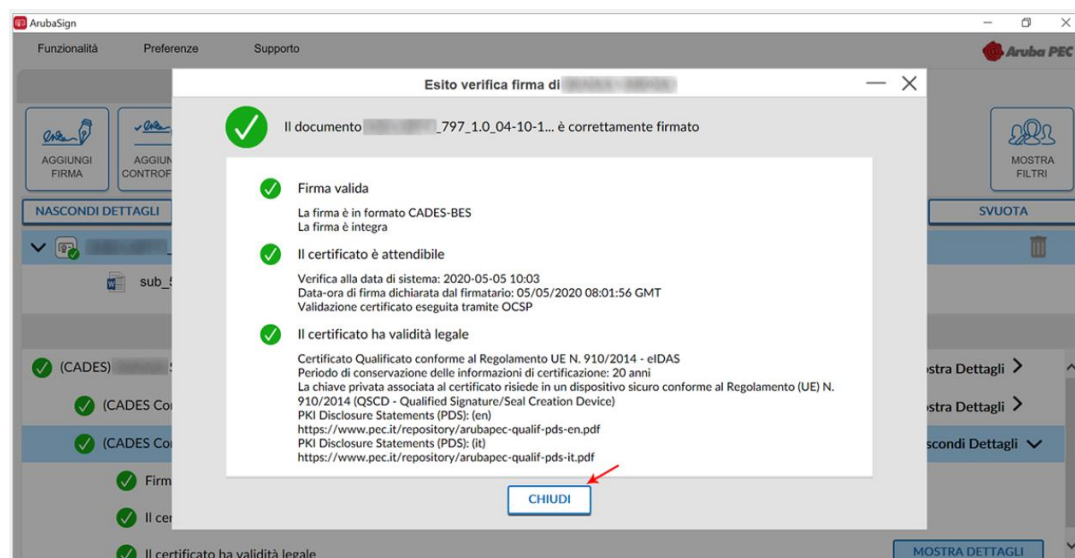
Firmare digitalmente il file. Il sistema non consente di selezionare il formato della Firma. In caso di File .p7m la **"Firma Parallela"** è apposta in tale formato, per i file .PDF è possibile apporre una Firma Grafica o Invisibile. **La nuova firma è apposta allo stesso livello di quella preesistente.**

18

È possibile visionare la presenza della Firma Parallela e i dettagli su **"MOSTRA DETTAGLI"** come da immagine esemplificativa sottostante:



E infine su **"MOSTRA DETTAGLI"** l'esito di verifica:



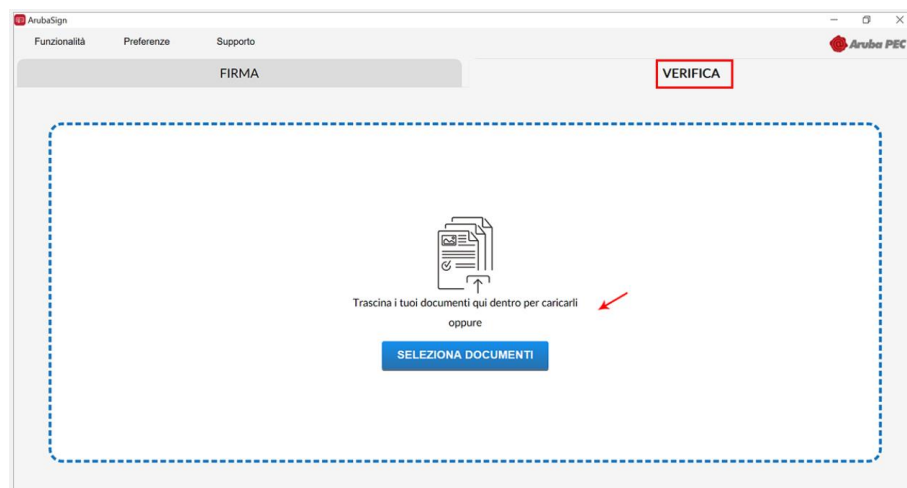
Affinché il documento informatico sottoscritto con Firma Digitale, produca gli effetti di legge di cui all'articolo 21, comma 2, del Codice dell'Amministrazione Digitale, il documento da firmare non deve contenere macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati. (Art. 3, comma 3 del DPCM 13 Gennaio 2004). È unicamente responsabilità dell'utente firmatario accertarsi che tale condizione sia soddisfatta. Ad esempio i file con estensione HTM o HTML sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Tali file, visualizzabili tramite qualsiasi Web Browser, possono contenere sia del codice interpretato (JavaScript, VBScript) che codice eseguibile (Applet Java, ActiveX ecc...) i quali ne forniscono una forte connotazione dinamica.

19

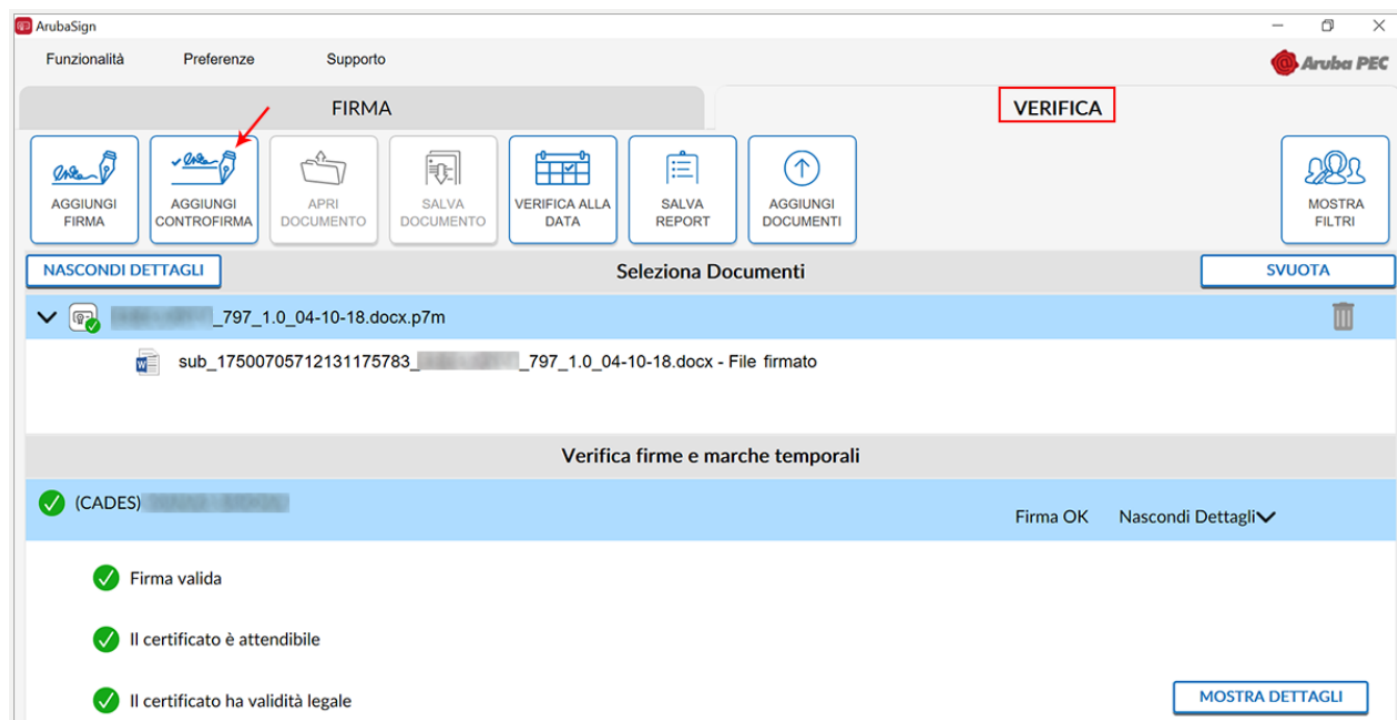
3.5 Apposizione "Controfirma" - Firma Remota

La funzione "Controfirma" è accessibile trascinando o selezionando il documento all'interno della scheda "VERIFICA" del Software Aruba Sign uno o più file già firmati in formato .p7m. È apposta a un livello sottostante di una firma preesistente e sottoscrive quest'ultima. È più annidata rispetto alla firma a cui si riferisce (aspetto evidenziato da una rappresentazione ad albero delle firme stesse).

Per crearla selezionare o trascinare un file .p7m (CADES), sopra il menù "VERIFICA" di Aruba Sign:



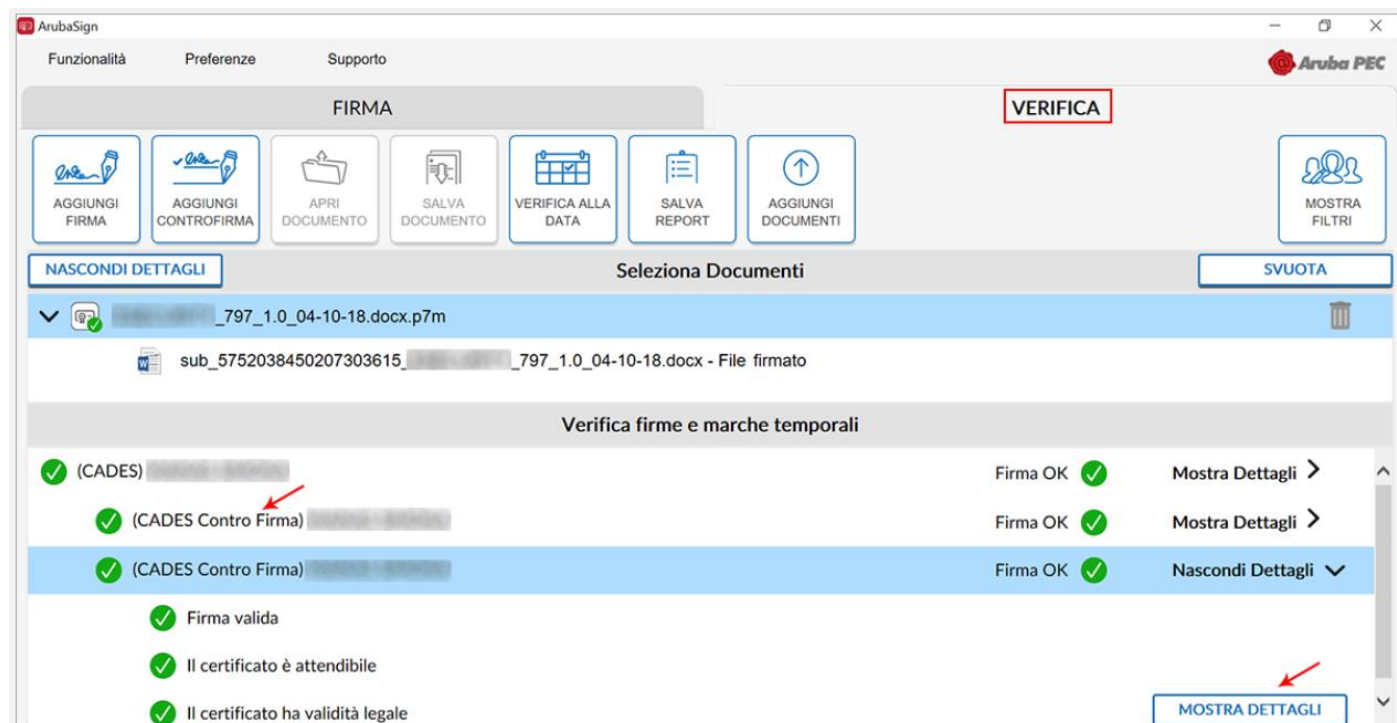
Selezionando il documento (anche in caso di caricamento di un solo file) su cui apporre la **Controfirma** cliccare su **"AGGIUNGI CONTROFIRMA"**:



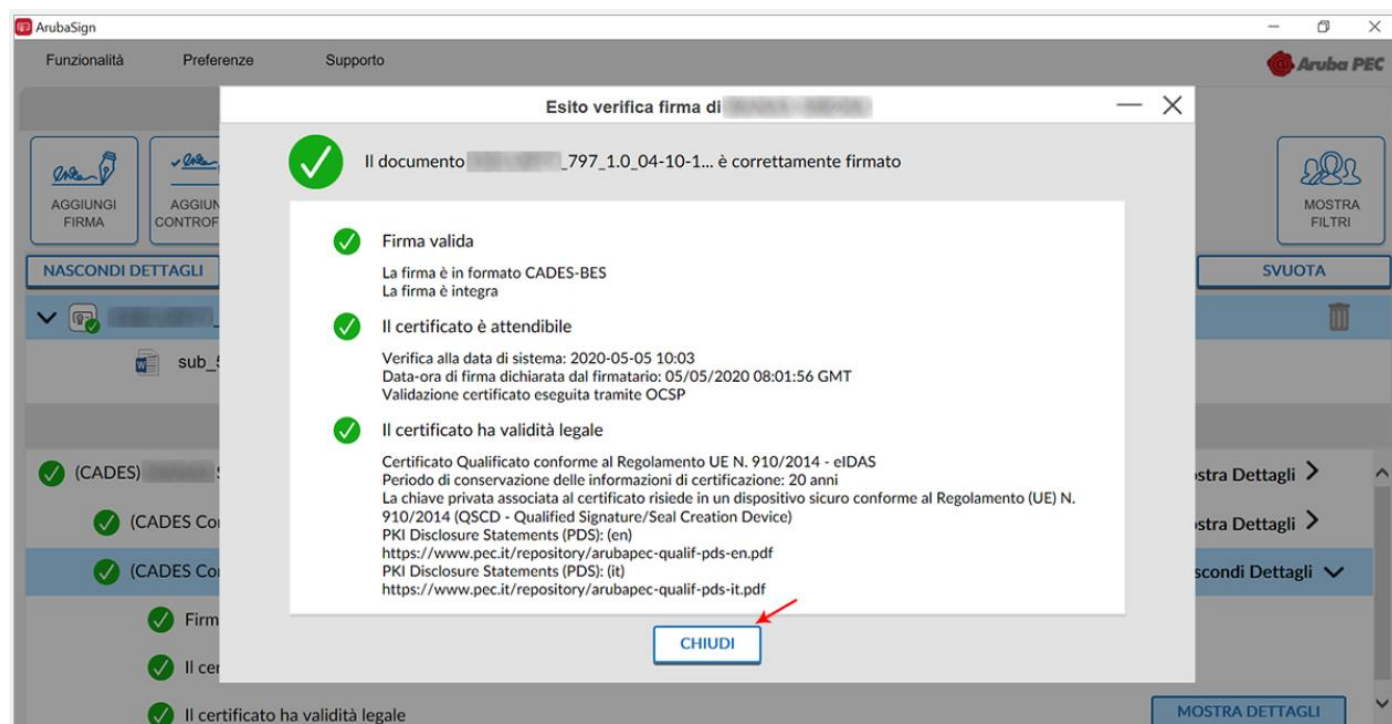
Firmare digitalmente il file in formato .p7m. La nuova Firma è apposta a un livello sottostante della firma preesistente.

È possibile visionare la presenza della Controfirma, come da immagine esemplificativa sottostante:

20



E infine su "**MOSTRA DETTAGLI**" l'esito di verifica firma:



Affinché il documento informatico sottoscritto con Firma Digitale, produca gli effetti di legge di cui all'articolo 21, comma 2, del Codice dell'Amministrazione Digitale, il documento da firmare non deve contenere macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati. (Art. 3, comma 3 del DPCM 13 Gennaio 2004). È unicamente responsabilità dell'utente firmatario accertarsi che tale condizione sia soddisfatta. Ad esempio i file con estensione HTM o HTML sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Tali file, visualizzabili tramite qualsiasi Web Browser, possono contenere sia del codice interpretato (JavaScript, VBScript) che codice eseguibile (Applet Java, ActiveX ecc.) i quali ne forniscono una forte connotazione dinamica.

21

3.6 Apposizione Firma PDF - Grafica (Firma Remota)

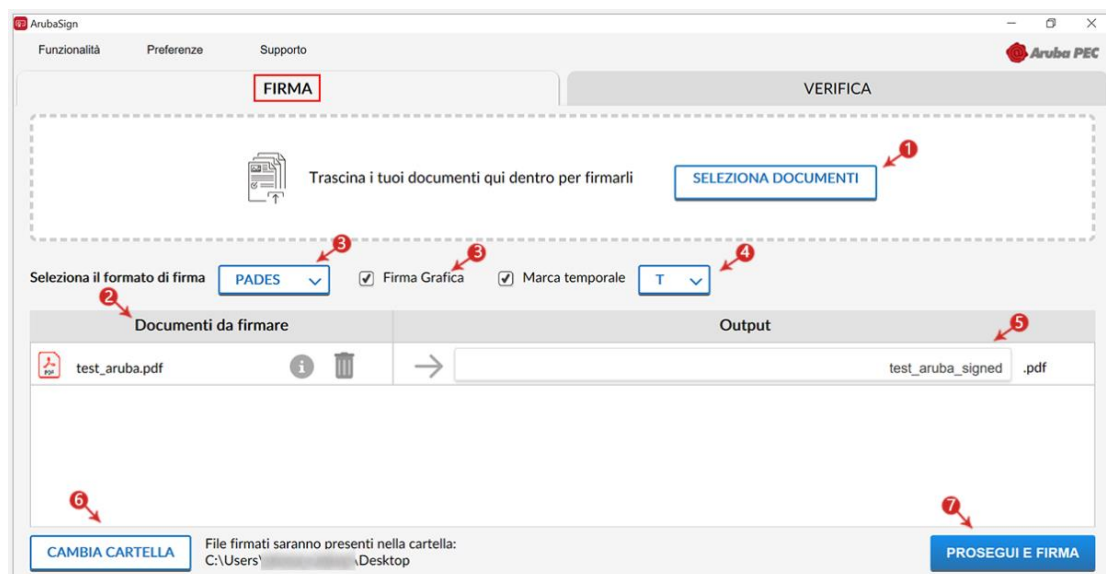
Il Formato di Firma **PADES** è applicabile ai soli file **.PDF**, **.doc**, **.docx**, **.xls**, **.xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

La Firma PADES - Firma Grafica permette di scegliere la posizione e la dimensione del campo che ospita la Firma Digitale.

Per firmare digitalmente uno o più file in formato **.PDF** in formato **PADES - Firma Grafica** e/o una intera cartella con **Aruba Sign e Firma Digitale Remota**:

- 1) Trascinare o selezionare **uno o più documenti e/o una intera cartella**;
- 2) Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
- 3) Dall'apposito menu a tendina "**Seleziona il formato di firma**" selezionare come tipologia di Firma "**PADES**" per firmare il file in formato **.PDF** e lasciare il Flag su "**Firma Grafica**";
- 4) Se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce "**Marca Temporale**" nel formato scelto dall'apposito menu a tendina;
- 5) Dalla finestra "**Output**" rinominare, se desiderato, eventuali file prima di apporre la firma;
- 6) Da "**CAMBIA CARTELLA**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;

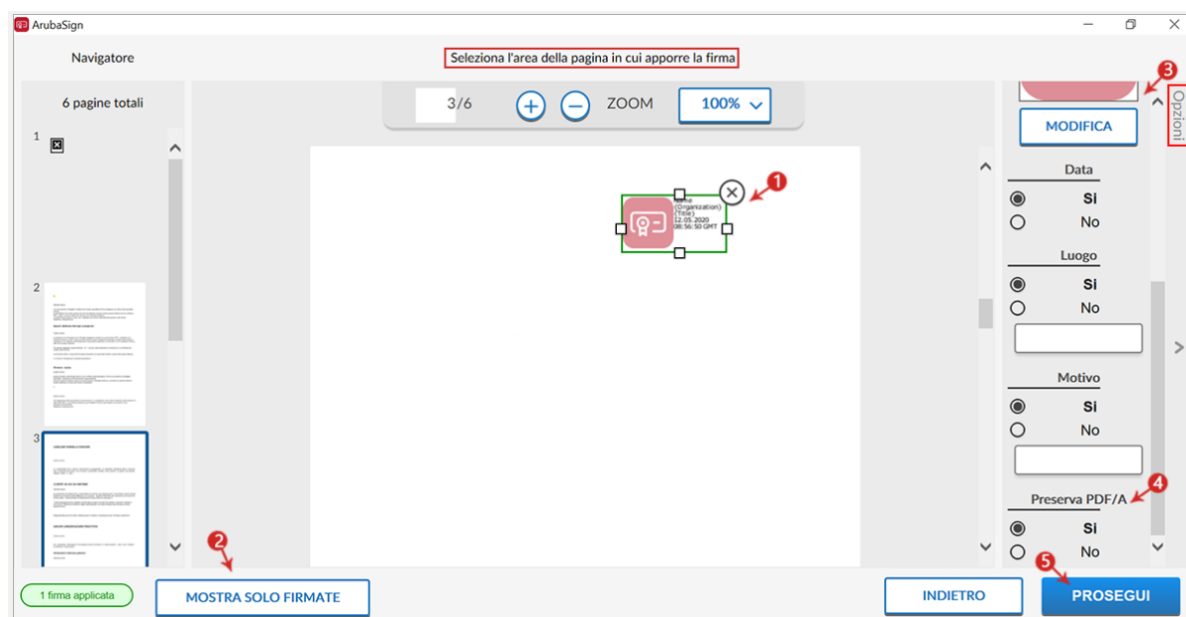
- 7) Cliccare su **"PROSEGUI E FIRMA"** per continuare. Sono firmati tutti i documenti presenti alla finestra **"Documenti da firmare"**:



Alla schermata successiva:

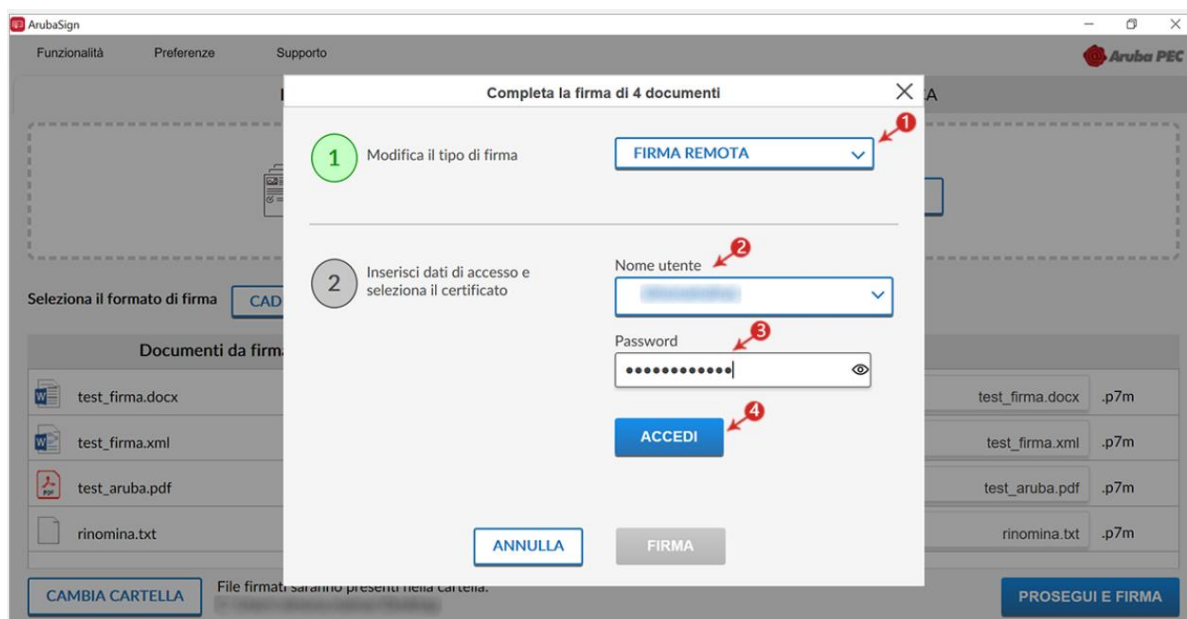
- 1) Definire la posizione e la dimensione del campo che ospiterà la Firma Digitale;
- 2) È possibile visualizzare tutti i documenti o solo quelli firmati;
- 3) Attraverso la finestra **Opzioni** sulla destra, è possibile caricare da locale, attraverso il tasto **MODIFICA**, una img in formato .gif/.jpg/.png da sostituire a quella presente di default per il timbro. L'immagine caricata è ridimensionata in scala rispetto alle dimensioni dell'area selezionata;
- 4) Abilitando la funzione **"Preserva PDF/A"** la firma grafica è apposta preservando il formato stesso;
- 5) Cliccare su **"PROSEGUI"** per procedere:

22



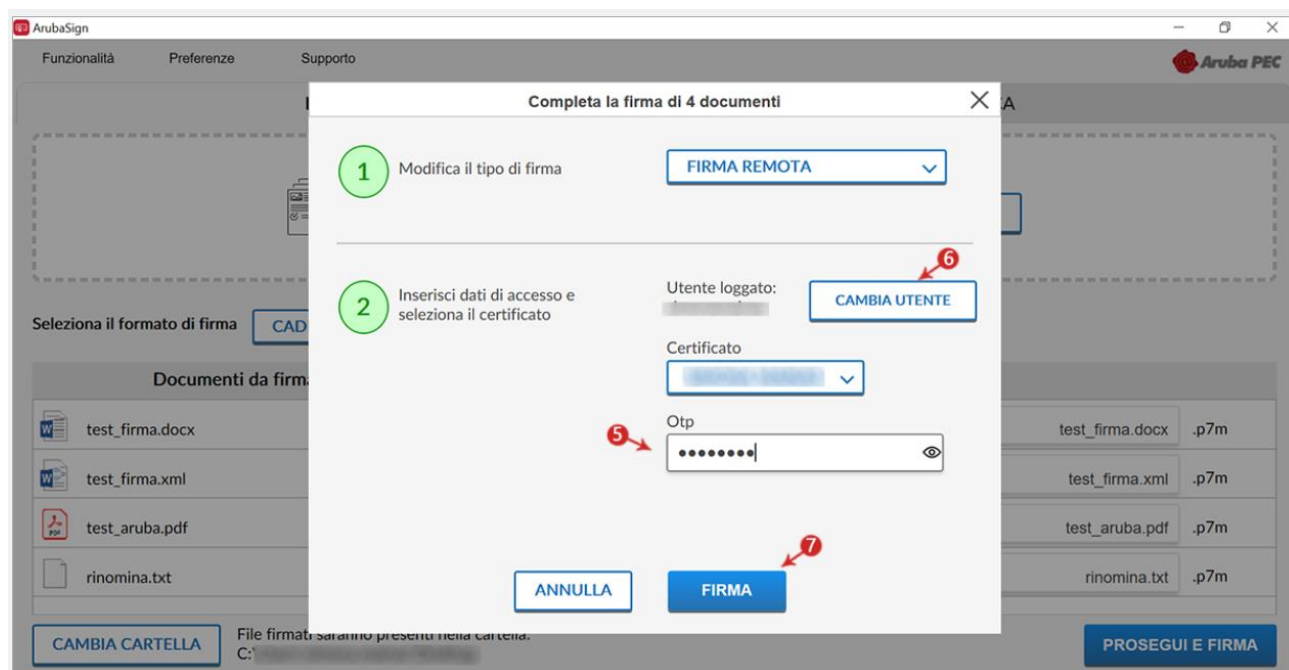
Alla schermata "Completa la firma di 4 documenti":

- 1) Selezionare o modificare il **tipo di firma**;
- 2) Inserire i dati di accesso "**Nome e utente**" del proprio account di Firma Digitale Remota;
- 3) Inserire la "**Password**" del proprio account di Firma Digitale Remota;
- 4) cliccare su "**ACCEDI**" e proseguire:

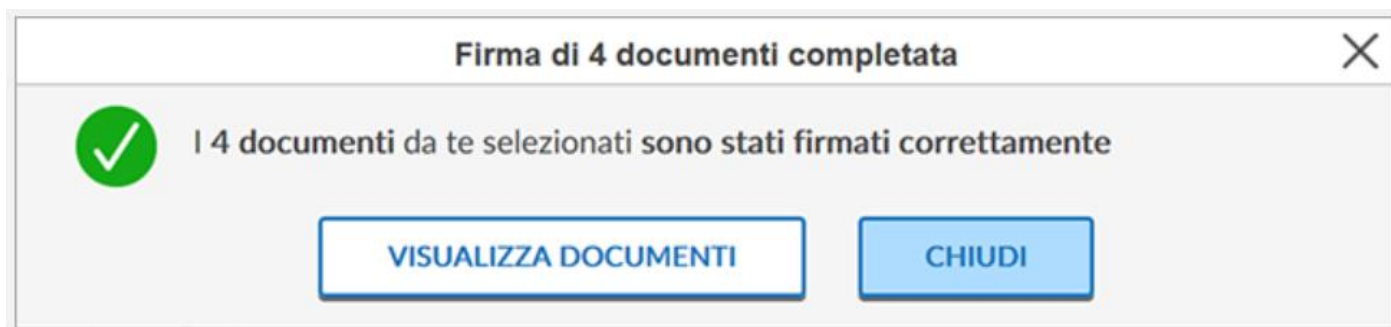


23

- 5) Inserire un **codice OTP** generato con il proprio dispositivo di Firma Digitale Remota;
- 6) Cliccando su "**CAMBIA UTENTE**" è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
- Cliccare su "**FIRMA**" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**CHIUDI**" per concludere:



Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al **nome originale** l'**estensione "signed.pdf"**.

3.7 Apposizione Firma PDF - Invisibile (Firma Remota)

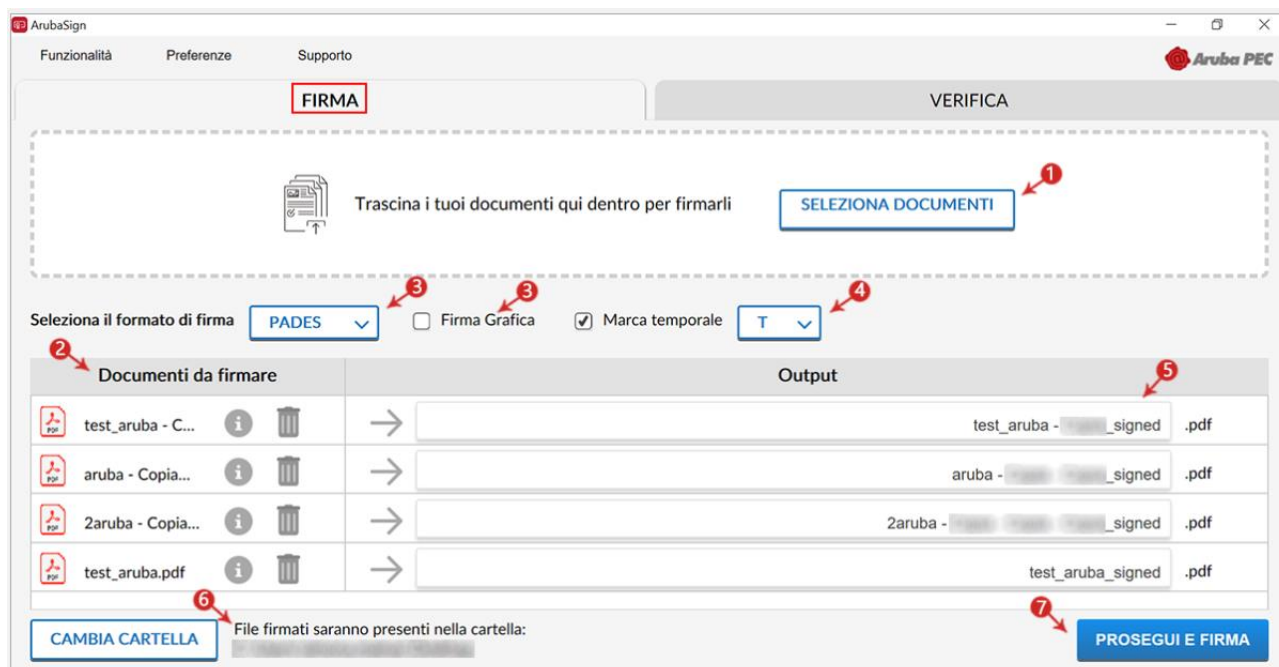
Il Formato di Firma **PAdES** è applicabile ai soli file **.PDF, .doc, .docx, .xls, .xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

La **Firma PAdES - Firma Invisibile** consente di evitare l'inserimento dell'"**appearance**" (**campo firma visibile**) all'interno delle pagine del documento firmato.

Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Invisibile** e/o una intera cartella **con Aruba Sign e Firma Digitale Remota**:

- 1) **Trascinare o selezionare uno o più documenti e/o una intera cartella;**
- 2) Il **singolo/i documenti caricati/o** sono visibili all'apposita schermata "**Documenti da firmare**";
- 3) Dall'apposito menu a tendina "**Seleziona il formato firma**" selezionare come tipologia di Firma "**PAdES**" per firmare il file in formato .PDF e rimuovere il Flag su "**Firma Grafica**";
- 4) Se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce "**Marca Temporale**" nel formato scelto dall'apposito menu a tendina;
- 5) Dalla finestra "**Output**" rinominare, se desiderato, eventuali file prima di apporre la firma;
- 6) Da "**CAMBIA CARTELLA**" verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;

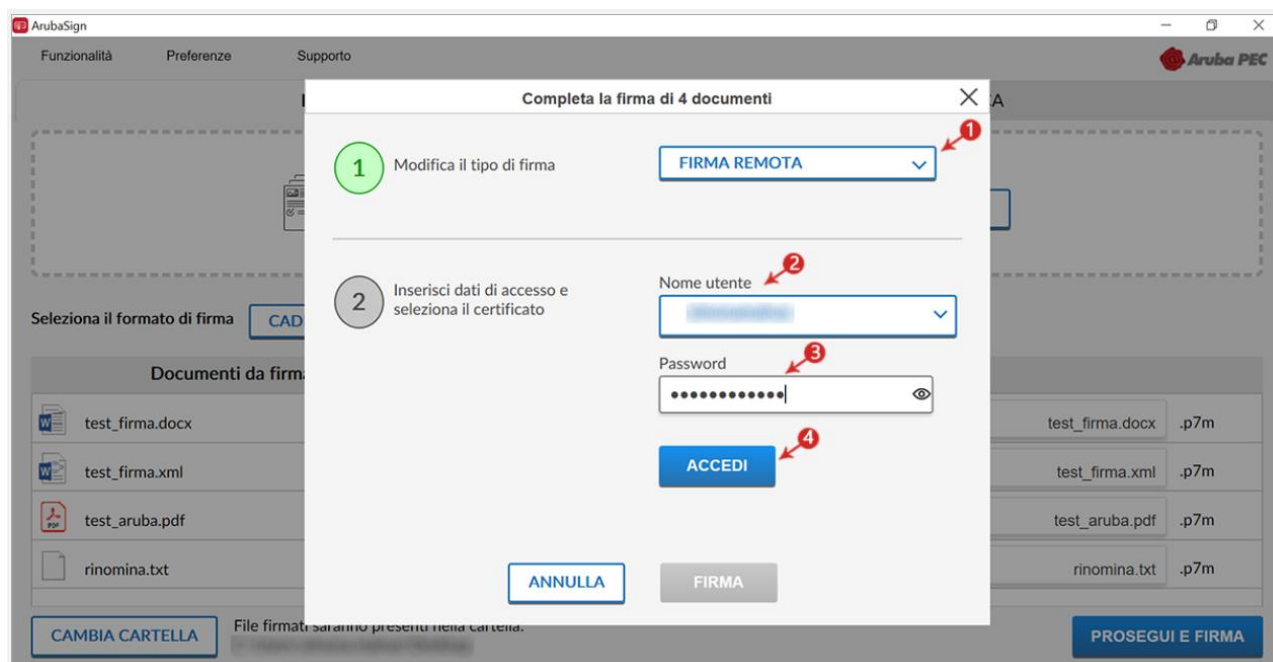
- 7) Cliccare su **"PROSEGUI E FIRMA"** per continuare. Sono firmati tutti i documenti presenti alla finestra **"Documenti da firmare"**:



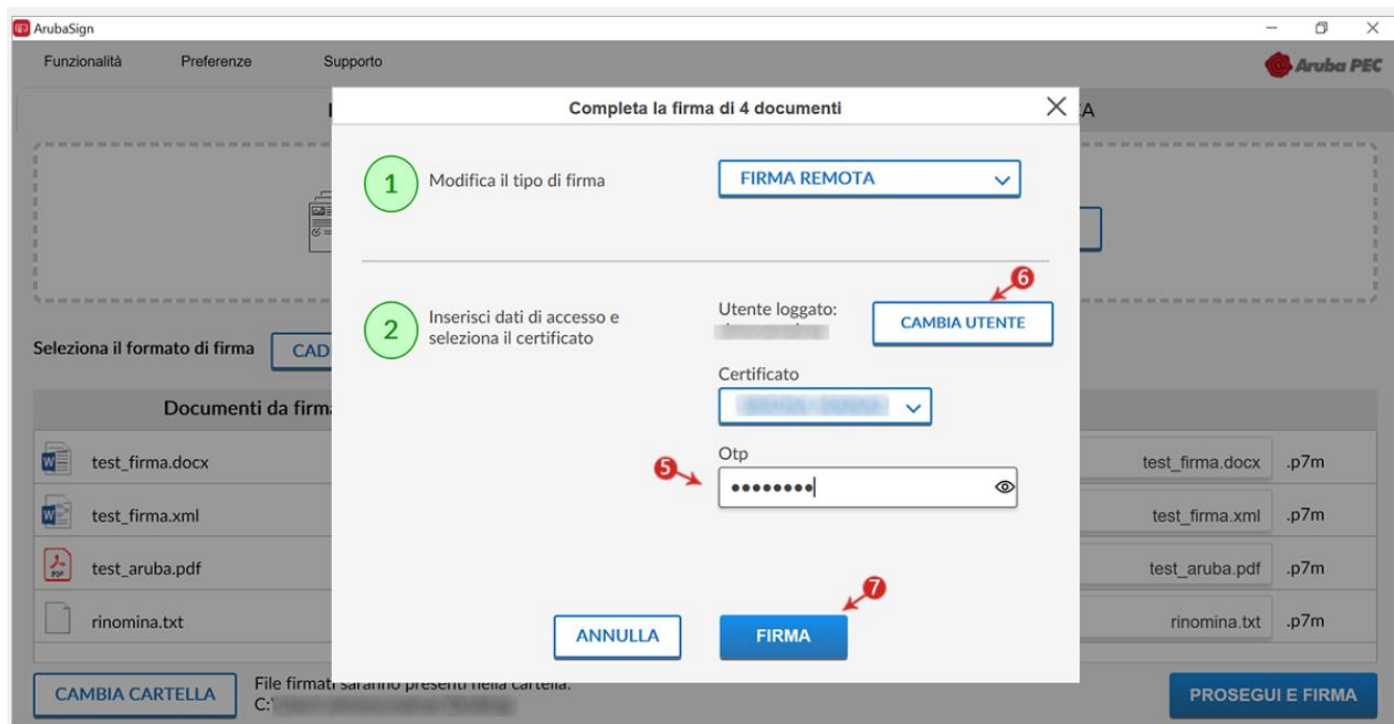
Alla schermata **"Completa la firma documenti"**:

- 1) Selezionare o modificare il tipo di firma;
- 2) Inserire i dati di accesso "Nome e utente" del proprio account di Firma Digitale Remota;
- 3) Inserire la "Password" del proprio account di Firma Digitale Remota;
- 4) Cliccare su **"ACCEDE"** e proseguire:

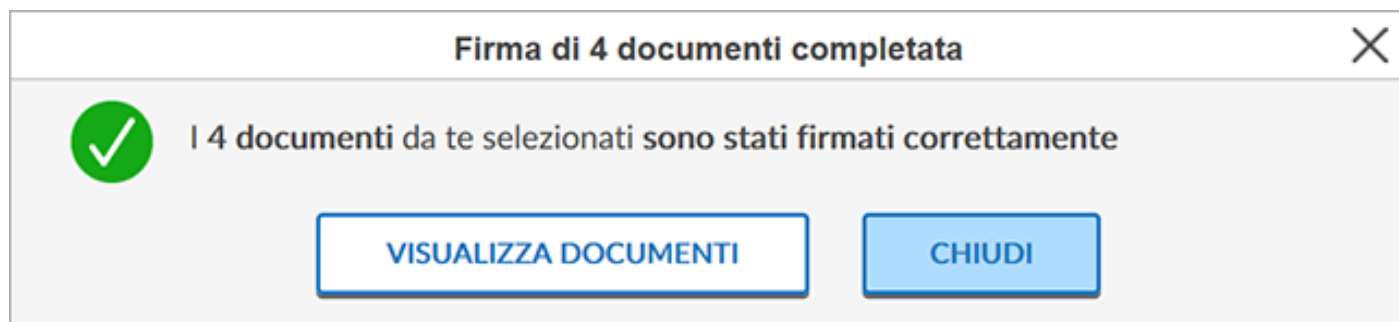
25



- 5) Inserire un codice OTP generato con il proprio dispositivo di Firma Digitale Remota;
- 6) Cliccando su "CAMBIA UTENTE" è possibile scegliere di firmare con altro account di Firma Digitale Remota configurato;
- 7) Cliccare su "FIRMA" per concludere il processo:



Al termine dell'operazione si visualizza la seguente schermata che notifica la corretta firma del file. Cliccare su "**CHIUDI**" per concludere:



Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al **nome originale** l'**estensione "signed.pdf"**.

3.8 Apposizione di Marche Temporalì - Firma Remota

La **Marca Temporale** permette di:

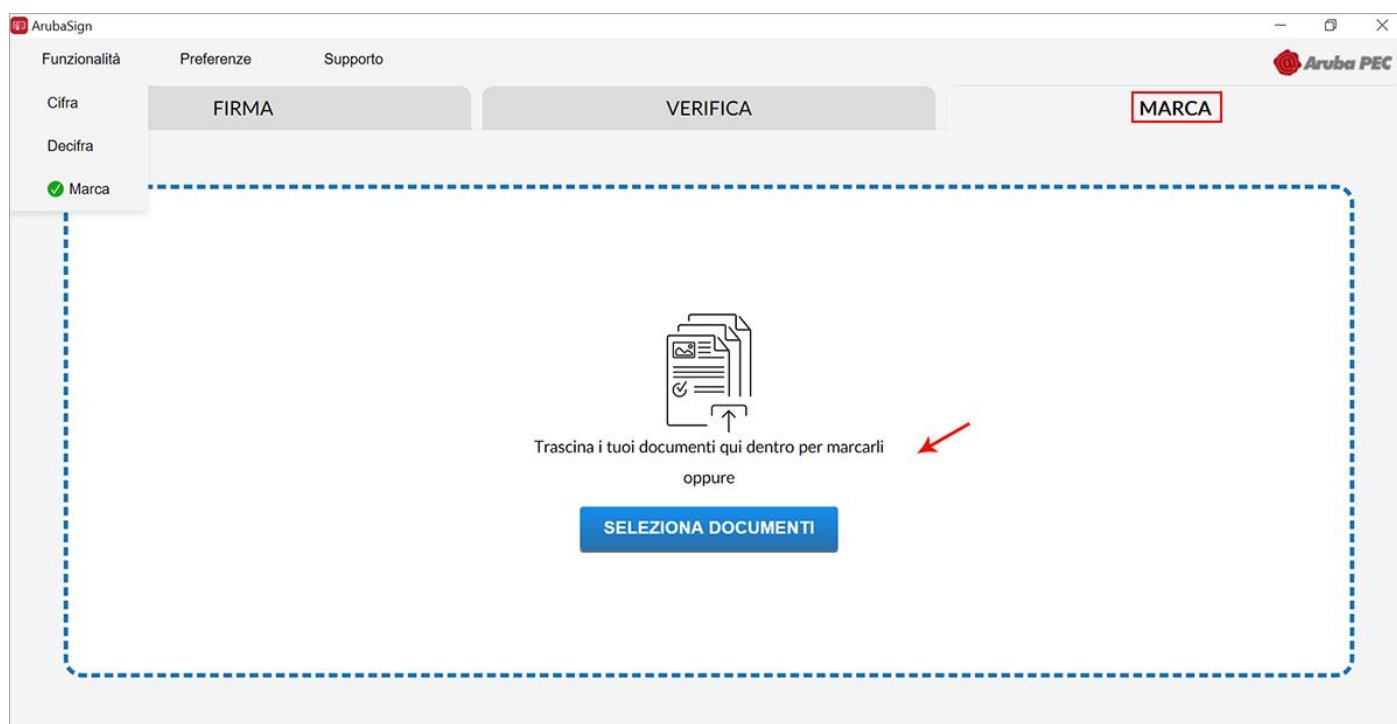
- **Associare data e ora certe e legalmente valide a un documento informatico**, attestando il preciso momento temporale in cui il documento è stato creato, trasmesso o archiviato;

- **Garantire la validità nel tempo del documento firmato digitalmente su cui è apposta**, poiché fa sì che la Firma Digitale risulti sempre e comunque valida anche nel caso in cui il relativo Certificato risulti scaduto, sospeso o revocato, **purché la Marca sia stata apposta in un momento precedente alla scadenza, revoca o sospensione del Certificato di Firma stesso.**

In caso di prima marcatura di un documento con il Software Aruba Sign, procedere prima alla configurazione di un proprio Account e successivamente alla marcatura stessa.

Apposizione di Marche Temporalì con Aruba Sign e un Dispositivo di Firma Digitale

Per apporre una marca temporale è sufficiente accedere su "**Funzionalità**" e poi su "**Marca**", se non precedentemente configurato verrà popolato sulla destra la scheda, quindi trascinare o selezionare il file che si desidera cifrare:



27

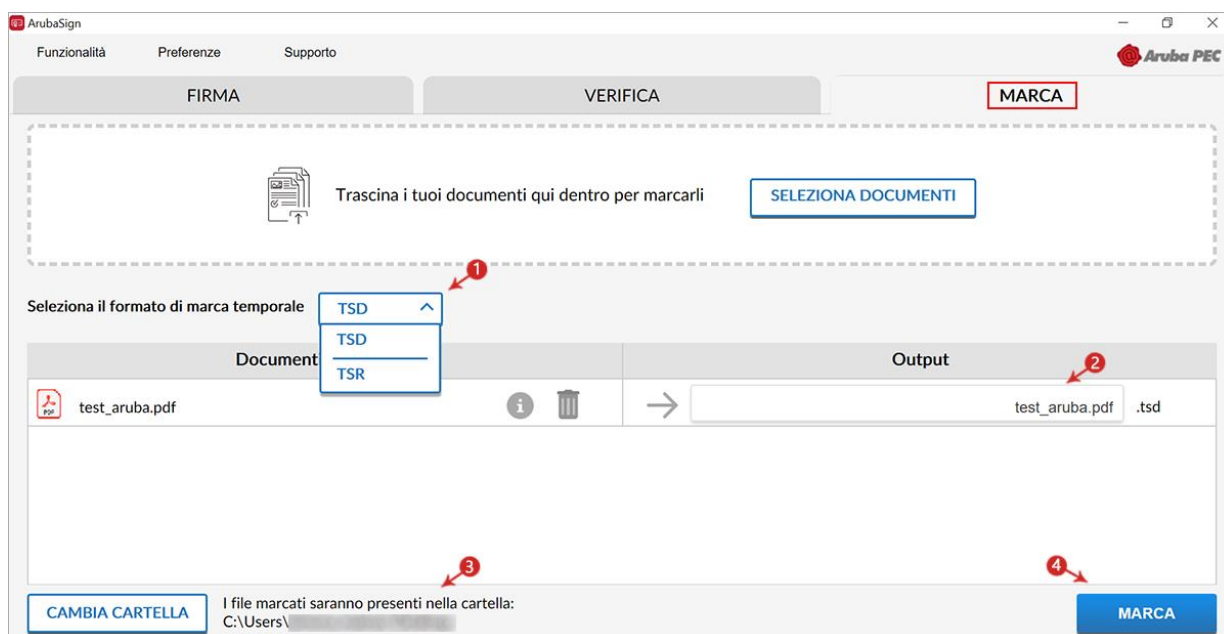
Alla pagina visualizzata:

- 1) Selezionare il formato di salvataggio della marca temporale. È possibile scegliere tra:
 - **TSR**: Il File creato contiene solo l'impronta del file, non tutto il file, e **la marca temporale in formato TSR è separata dal documento**. Pertanto, per verificare il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Se si appone una marca temporale in formato TSR e si desidera inviarla a un destinatario, è necessario inviare anche il documento di origine.
 - **TSD**: Il File creato comprende sia **il file sottoposto a marcatura che la marcatura temporale stessa**. Se si appone una marca temporale in formato TSD e si desidera inviarla a un destinatario, non è necessario inviare anche il documento di origine.

Gli altri dati (password e cartella di destinazione del file) sono indicati automaticamente dal sistema:

- La **password** è preimpostata a seguito della configurazione dell'Account di marcatura Temporale;
- Il **percorso di destinazione del File** inserito è la cartella su cui risiede il file originale.
- Dalla finestra "**Output**" rinominare, se desiderato, eventuali file prima di apporre la firma;
- Il documento è disponibile nella cartella indicata in fase di apposizione della marcatura stessa;

- Cliccare **"MARCA"** al messaggio che notifica la corretta marcatura del file per completare l'operazione:

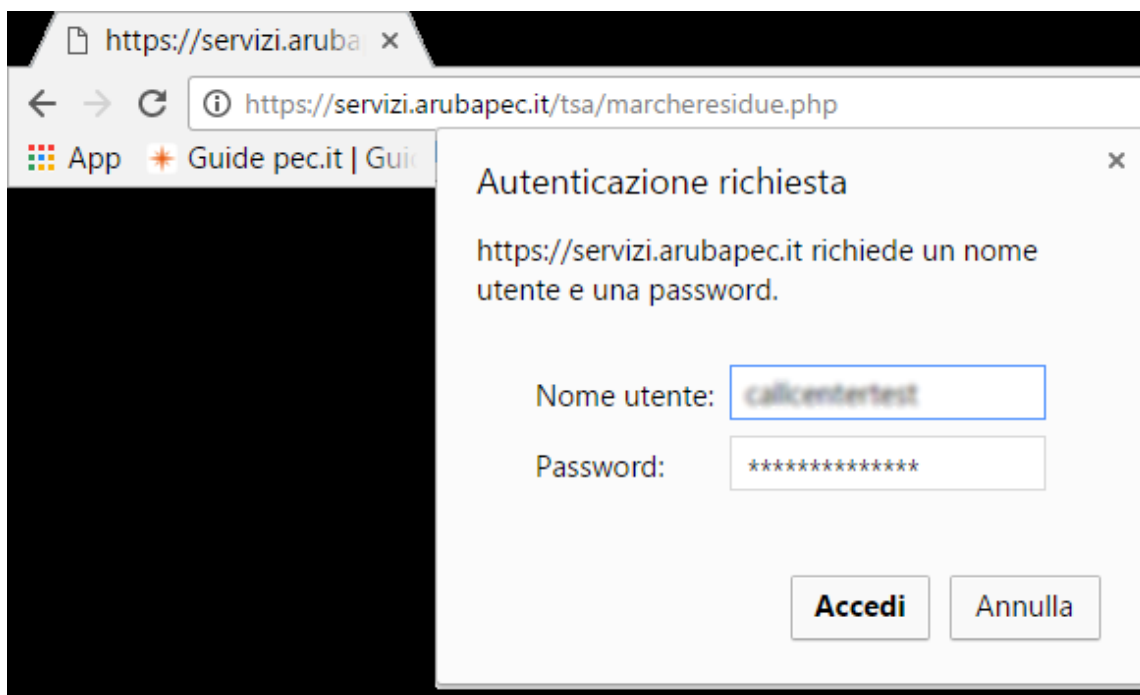


Verifica Marche Temporal Residue

Aruba Sign non indica il numero di marche di volta in volta utilizzate. Qualora si voglia verificare le marche residue:

28

- 1) Accedere a <https://servizi.arubapec.it/tsa/marcheresidue.php>;
- 2) Al Form visualizzato inserire le credenziali del proprio Account di marcatura temporale, quindi spuntare su "Ok":



Si accede alla pagina da cui visualizzare le marche residue:

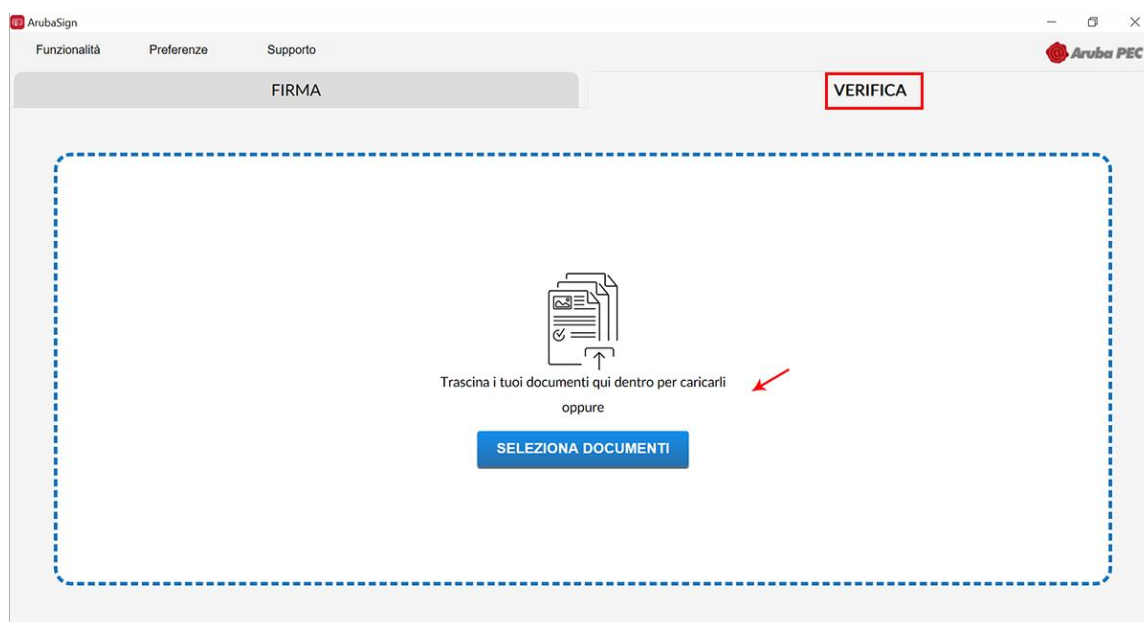


L'**apposizione della Marca Temporale** a un documento firmato digitalmente o meno, con **Aruba Sign**, può avvenire solo ed esclusivamente a seguito [dell'acquisto](#) di un lotto di marche temporali e alla configurazione di un proprio Account.

29

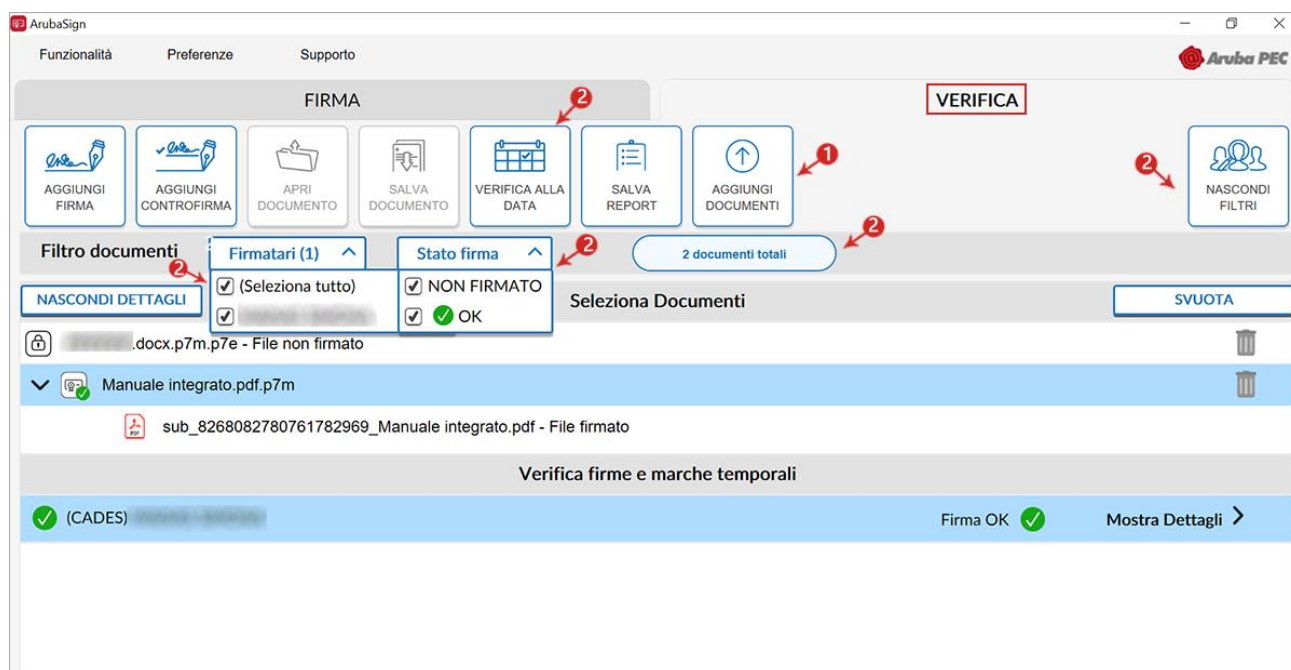
3.9 Verifica di File Firmati (Aruba Sign e Firma Remota)

La **Verifica dei File firmati** permette di verificare la **validità legale del certificato**. Per verificare uno o più file firmati con Aruba Sign, selezionare il documento nella scheda **"VERIFICA"**:



Alla schermata visualizzata è possibile:

- 1) Verificare ulteriori file firmati trascinandoli da locale o su **"AGGIUNGI DOCUMENTO"**;
- 2) Da **"Mostra/Nascondi Filtri"** sono riportati il nome e cognome del/i firmatario/i, il numero di firme che ha apposto, la data dell'ultima apposizione e lo "Stato" (esito) della verifica. Per visionare quali sono i documenti firmati da uno specifico firmatario, inserire il flag in corrispondenza del soggetto interessato, il nome appare a fianco dei singoli file che ha firmato presenti nell'area "Seleziona documenti":



- 3) **"Verifica firme e marche temporali"** sono visibili le firme presenti all'interno del file:

- **Firma valida**

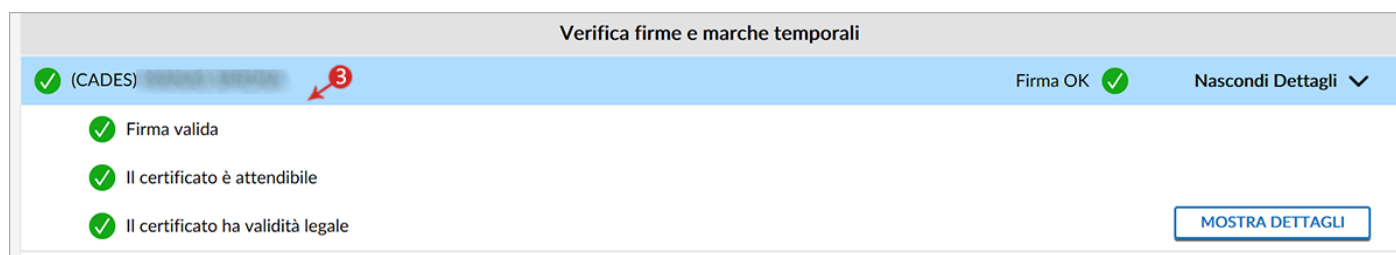
Attesta il formato della firma e che il documento non è stato alterato dopo la firma;

- **Il certificato è attendibile**

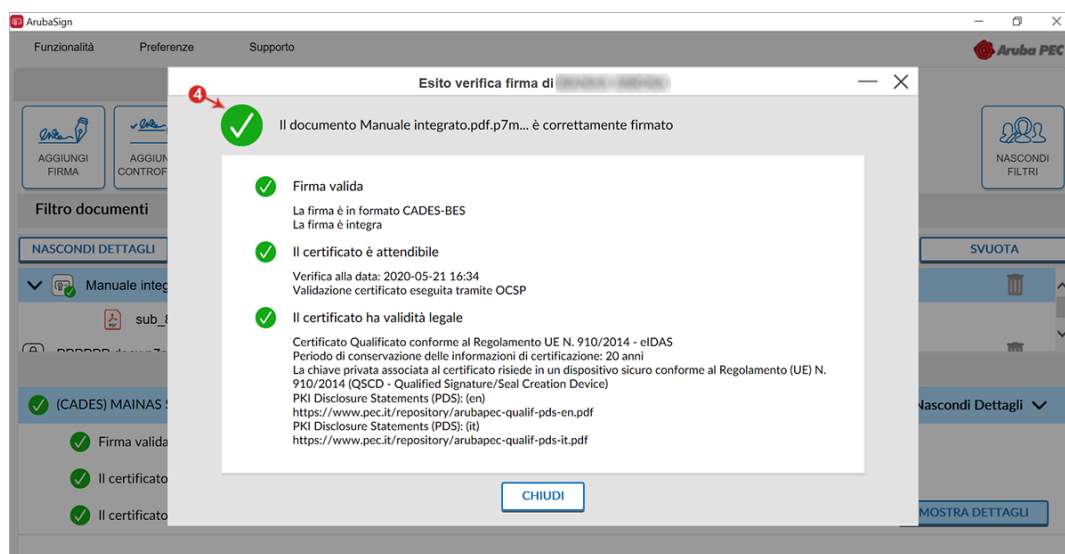
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della Verifica;

- **Il certificato ha validità legale**

Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



4) Da "Mostra Dettagli" è possibile verificare la validità della firma apposta:



Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "Firma KO", attestante che sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta, ma qualcuno non è andato a buon fine.

In caso di necessità è possibile attivare un'opzione che consente di verificare uno o più File Firmati con certificati non emessi da una Certification Authority. La verifica della Firma opposta può essere:

Non qualificata: la firma è considerata valida se è integra e il certificato valido. Non è richiesto che sia emesso da una Certification authority di firma digitale.

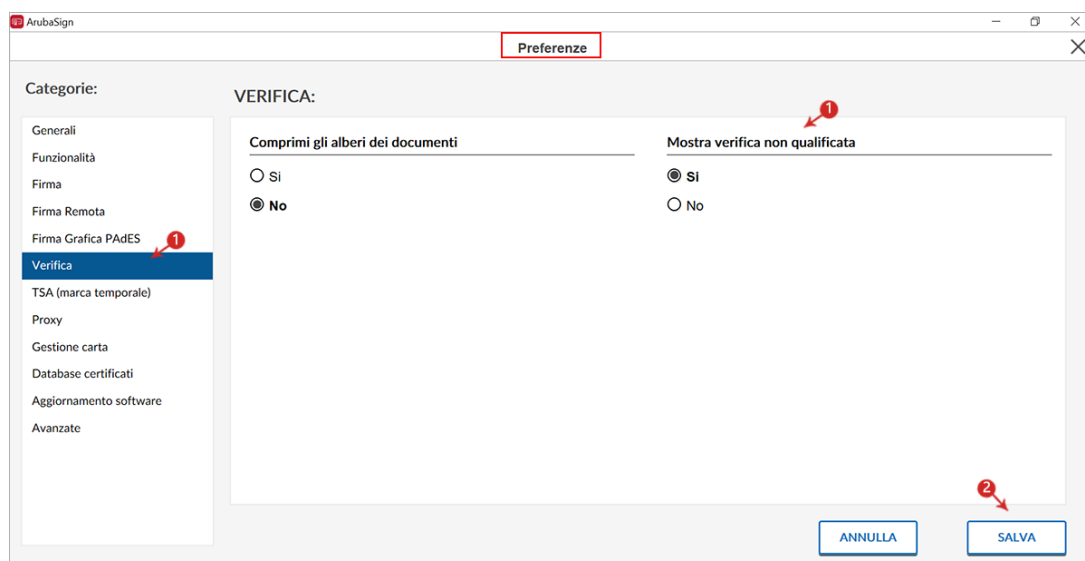
Qualificata: la firma apposta a un file è considerata valida se è integra, il certificato valido e rilasciato da una Certification Authority qualificata nel rispetto della normativa vigente circa la firma digitale qualificata.

La Firma "Non Qualificata" non ha la stessa validità legale della Firma "Qualificata".

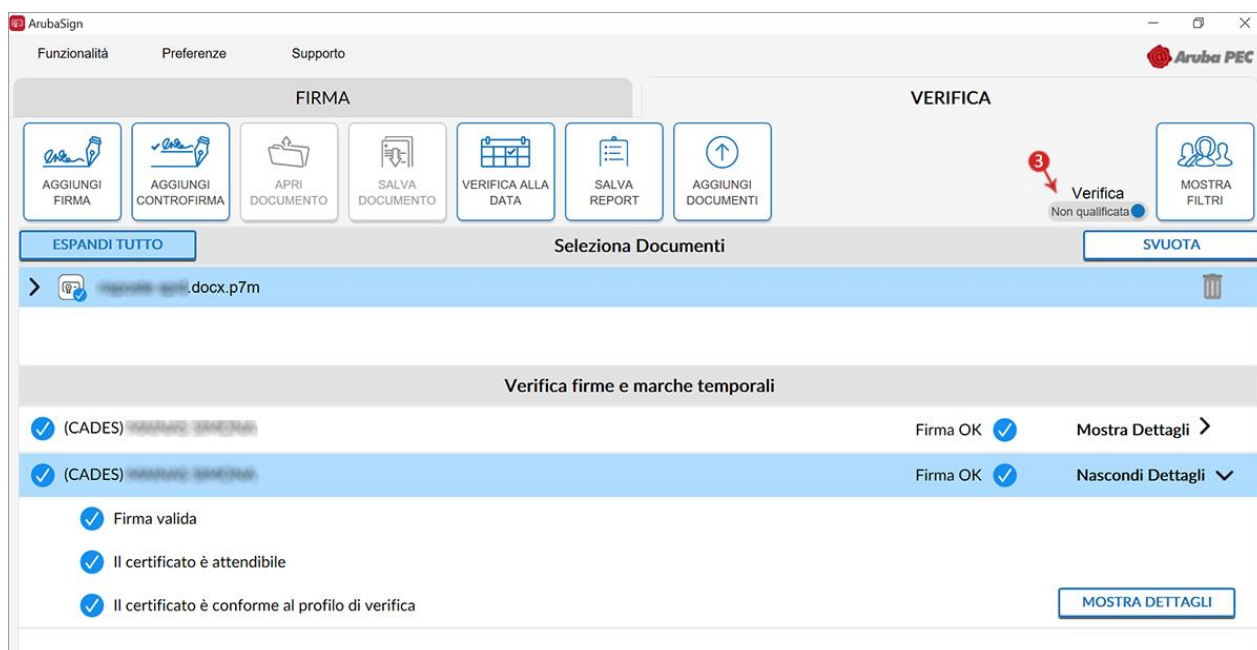
Per attivare l'opzione, accedere su "Preferenze" di Aruba Sign:

Su "VERIFICA" abilitare "Mostra verifica non qualificata";

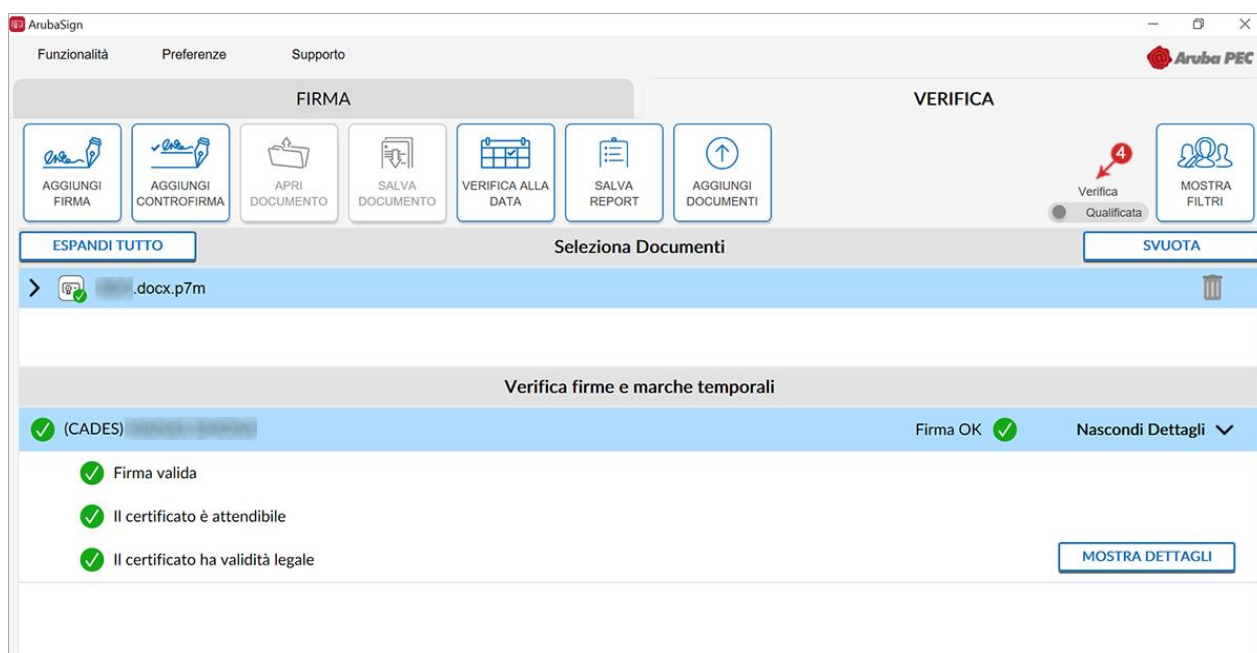
Confermare su "SALVA":



1) L'opzione di verifica **"Non qualificata"** è attiva:



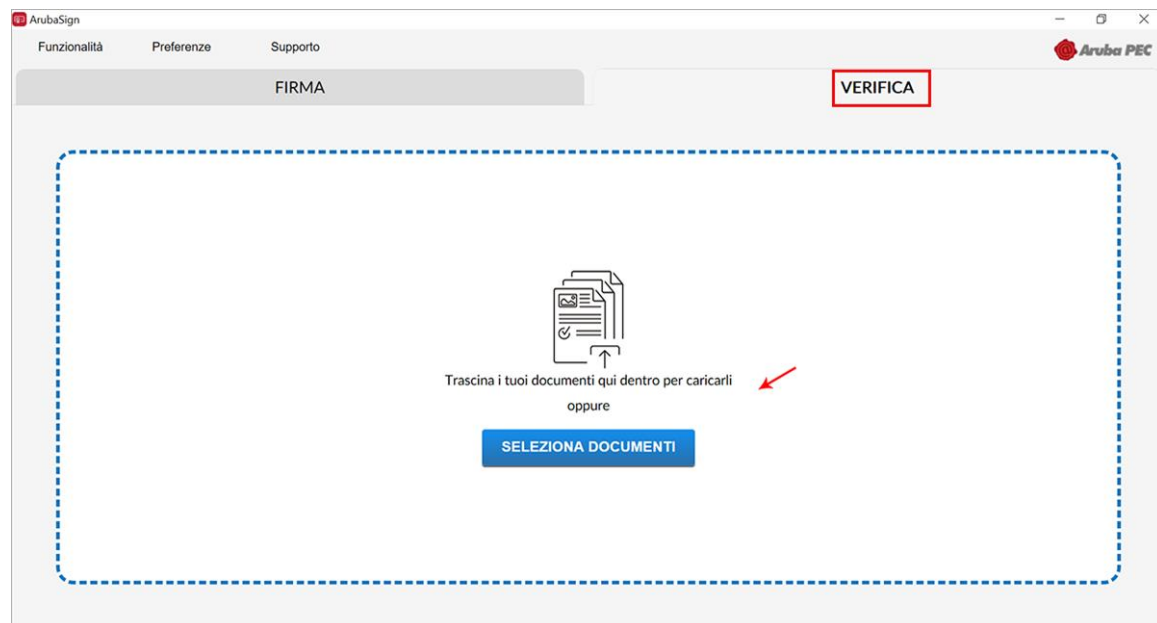
2) Se l'opzione non viene attivata, la verifica è **"Qualificata"**:



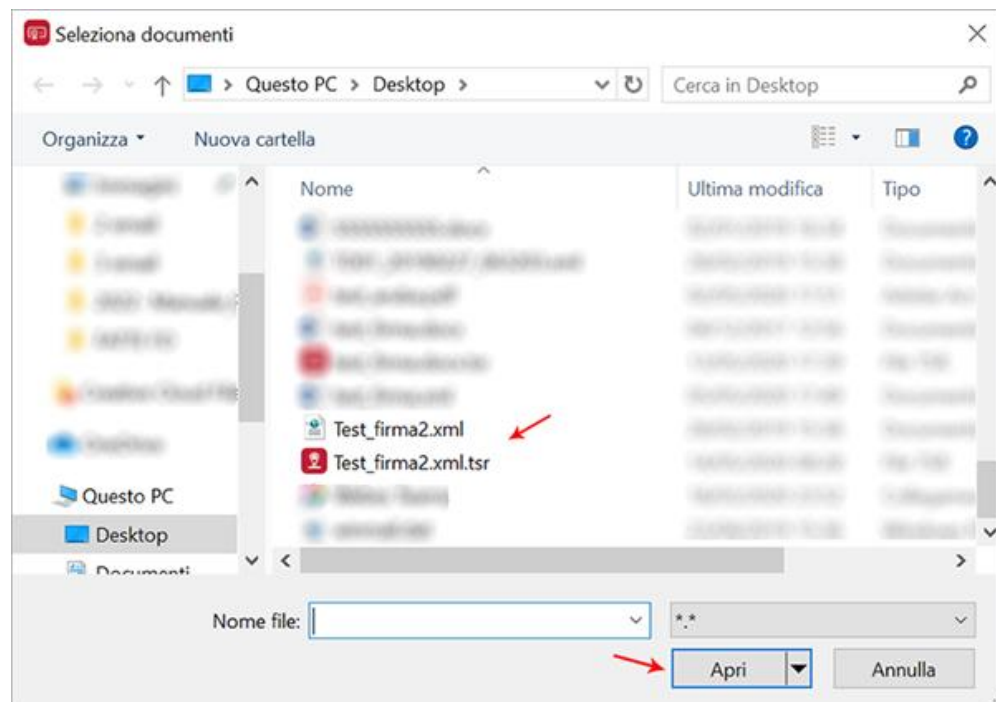
L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In **Italia**, nel periodo estivo (ora "legale"), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora "solare") l'orario è avanti di un'ora sulla UTC.

3.10 Verifica di marca temporale in Formato TSR (Aruba Sign e Firma Remota)

Una marca temporale in formato **TSR** è **separata dal documento su cui è apposta**. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Per **verificare uno o più File marcati in formato TSR con Aruba Sign**, trascinare o selezionare il documento all'interno della scheda **"VERIFICA"**:



Selezionare da locale il file originario e il file associato alla marca stessa, quindi cliccare su **"Apri"**:



Alla schermata visualizzata è possibile:

- 1) Visualizzare il file marcato;
- 2) Su **"Verifica firme e marche temporali"** sono visibili le marche presenti all'interno del file:

- **Marca valida**

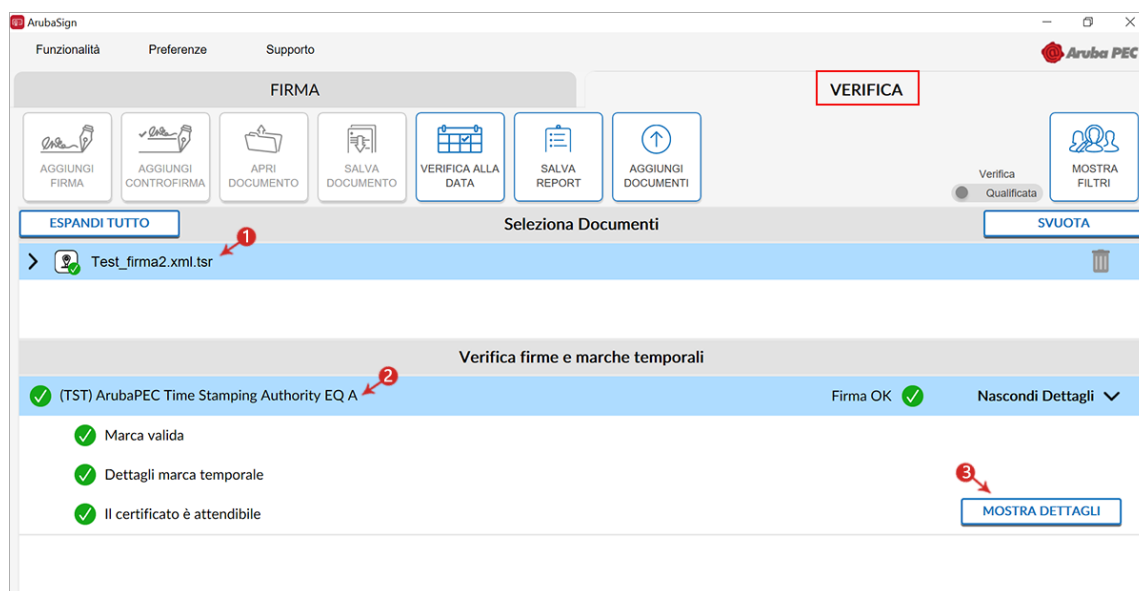
Indica che la marca temporale è integra ed è correttamente associata al documento selezionato, nella parte **"Dettagli marca temporale"**, sono riportate le specifiche della marca stessa;

- **Dettagli marca temporale**

Sono riportate le specifiche della marca stessa;

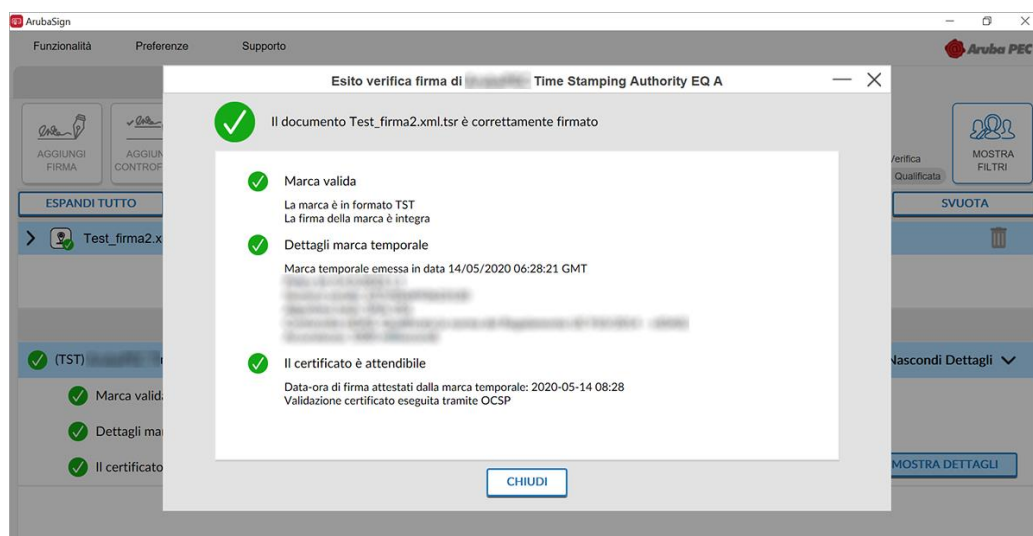
- **Il certificato è attendibile**

Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori:



34

- 3) Da **"MOSTRA DETTAGLI"** è possibile verificare la validità della firma apposta:



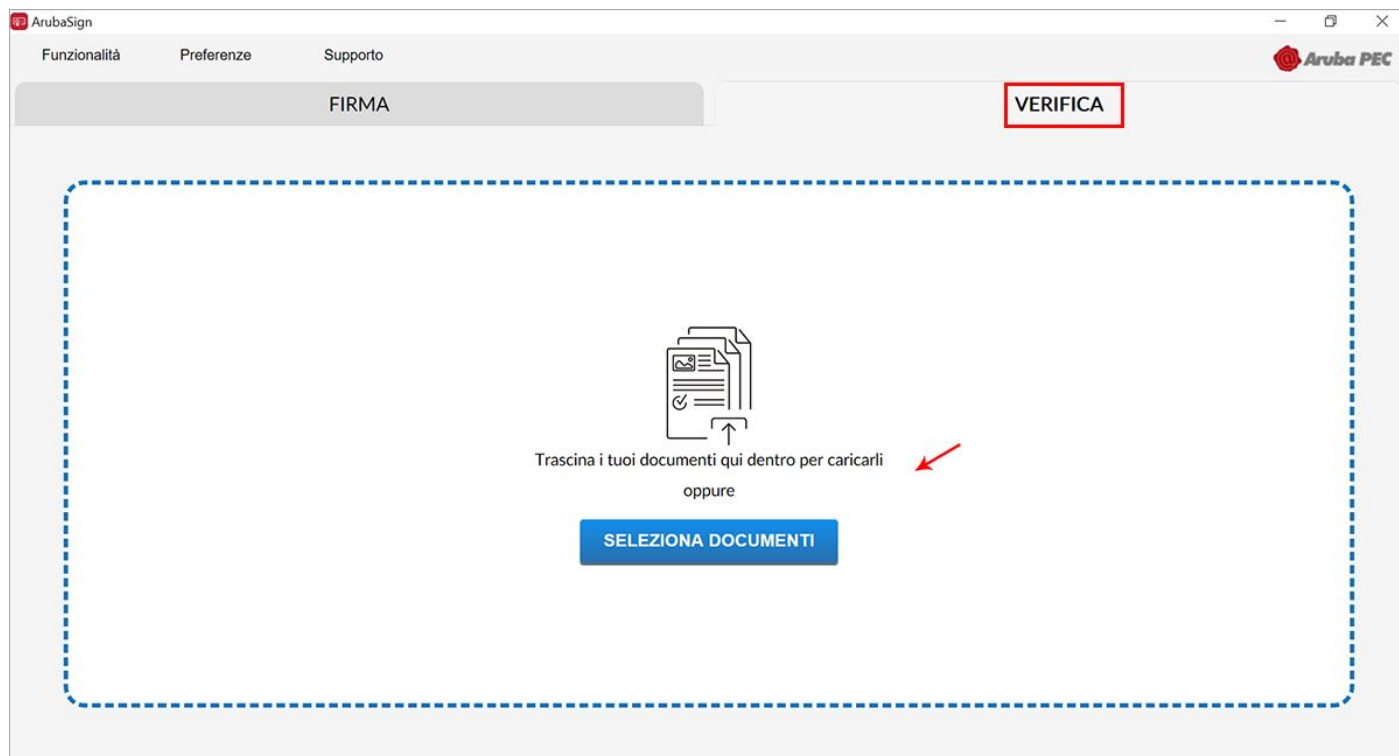
Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "Marca KO", attestante che **sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta, ma qualcuno non è andato a buon fine.**

L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In Italia, nel periodo estivo (ora "legale"), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora "solare") l'orario è avanti di un'ora sulla UTC.

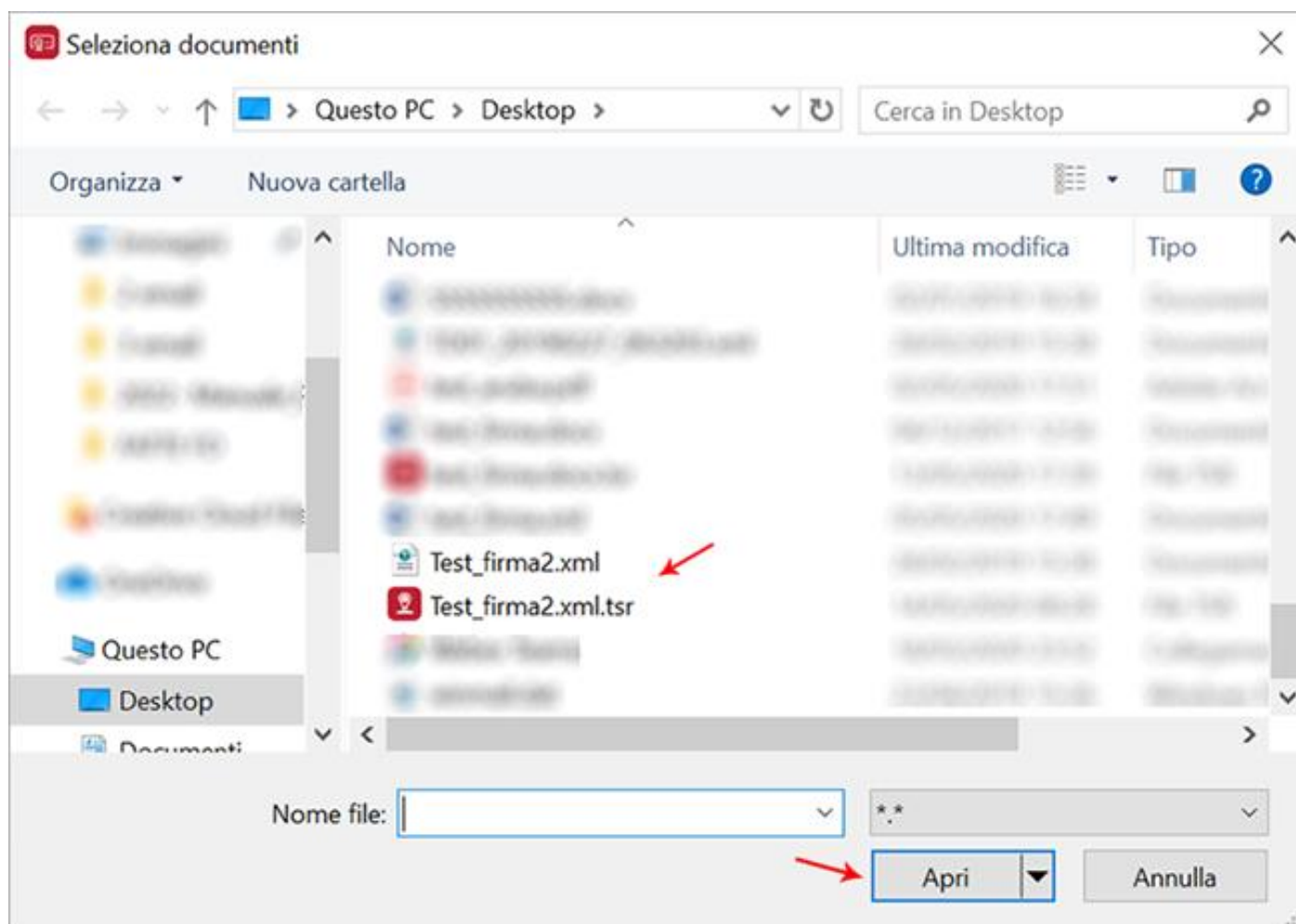
3.11 Verifica di marca temporale in Formato TSD (Aruba Sign e Firma Remota)

Una marca temporale in formato TSD comprende sia il file sottoposto a marcatura che la marcatura temporale stessa. Pertanto, per verifica il file TSD, non è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSD stesso.

Per verificare uno o più File marcati in formato TSD con Aruba Sign, trascinare o selezionare il documento all'interno della scheda "VERIFICA":



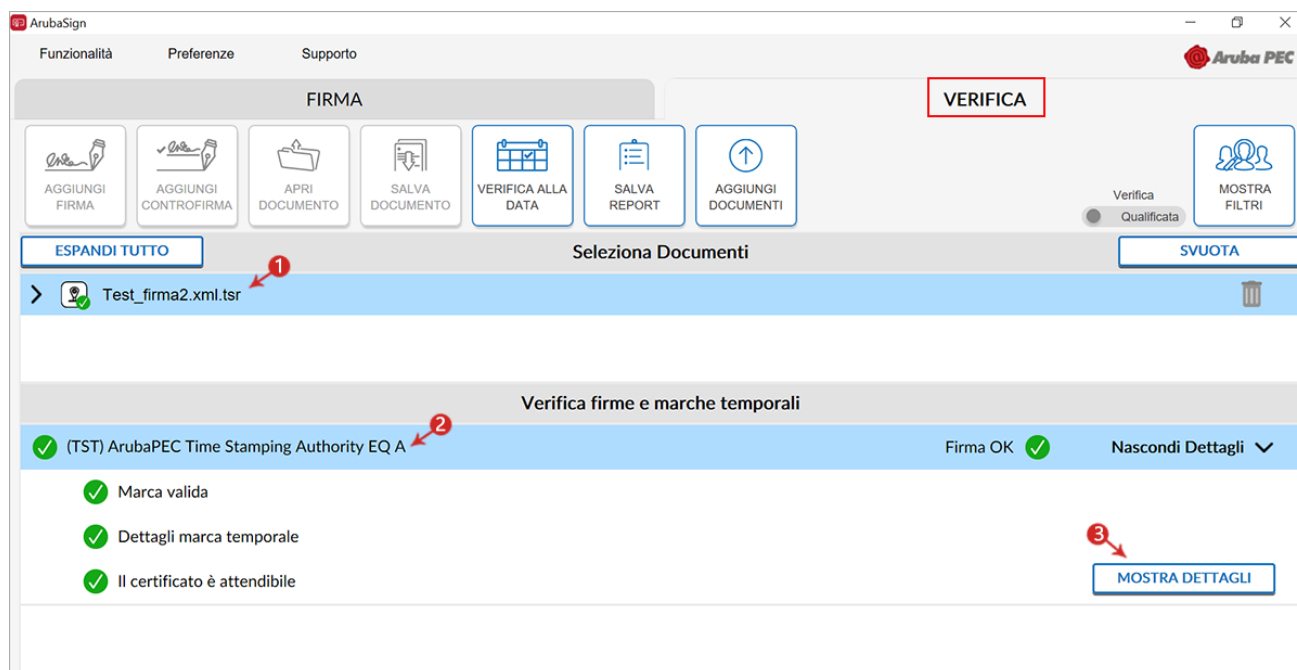
Selezionare da locale il file associato alla marca stessa, quindi cliccare su **"Apri"**:



36

Alla schermata visualizzata è possibile:

- 1) Visualizzare il file marcato;
- 2) Su **"Verifica firme e marche temporali"** sono visibili le marche presenti all'interno del file;
 - **Marca valida**
Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;
 - **Dettagli marca temporale**
Sono riportate le specifiche della marca stessa;
 - **Il certificato è attendibile**
Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori;
- 3) Da **"MOSTRA DETTAGLI"** è possibile verificare la validità della firma apposta:



ArubaSign

Funzionalità Preferenze Supporto

FIRMA VERIFICA

AGGIUNGI FIRMA AGGIUNGI CONTROFIRMA APRI DOCUMENTO SALVA DOCUMENTO VERIFICA ALLA DATA SALVA REPORT AGGIUNGI DOCUMENTI

ESPANDI TUTTO Seleziona Documenti SVUOTA

> Test_firma2.xml.tsr

Verifica firme e marche temporali

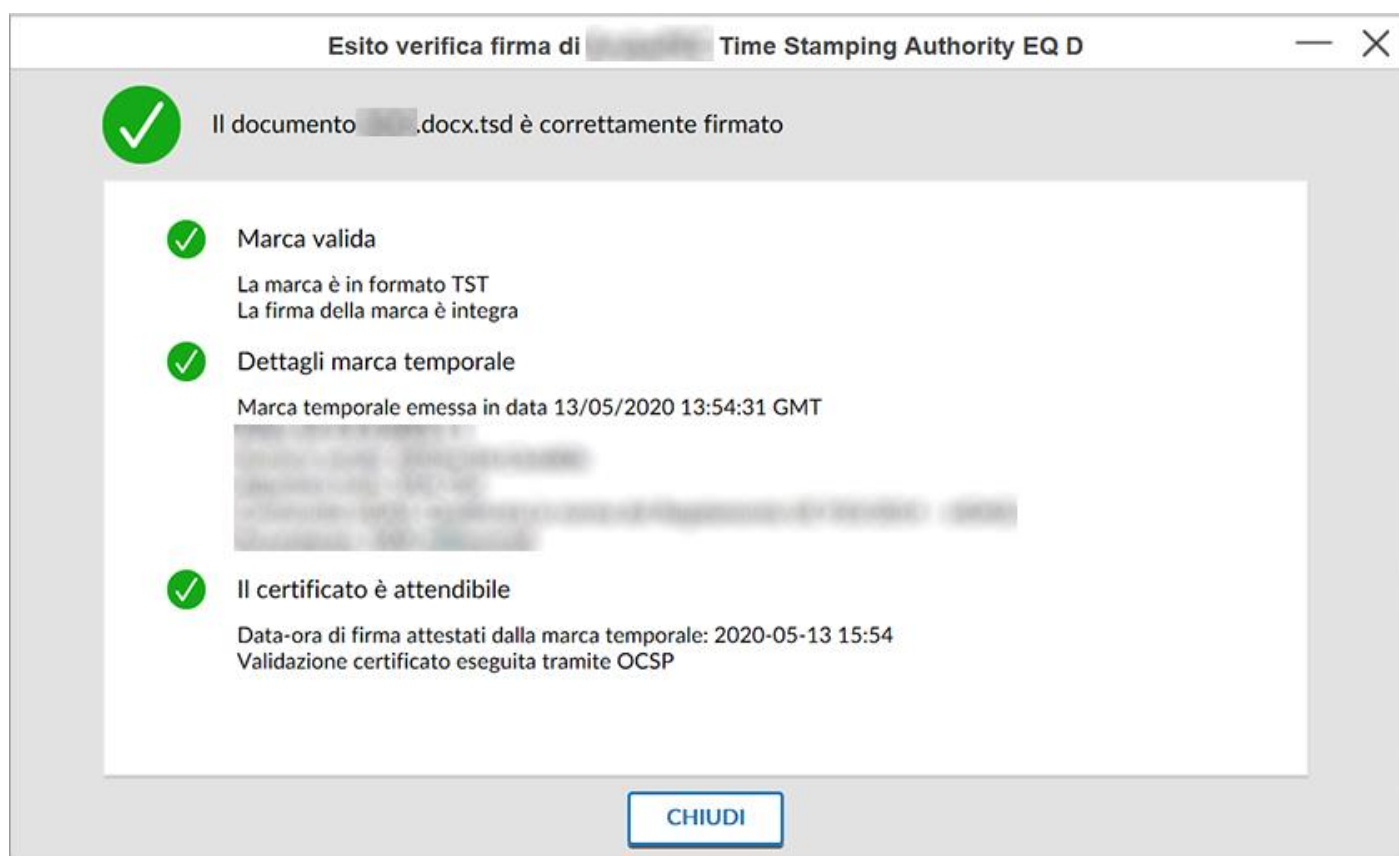
✓ (TST) ArubaPEC Time Stamping Authority EQ A Firma OK ✓ Nascondi Dettagli

✓ Marca valida

✓ Dettagli marca temporale

✓ Il certificato è attendibile

MOSTRA DETTAGLI



Esito verifica firma di Time Stamping Authority EQ D

✓ Il documento .docx.tsd è correttamente firmato

✓ Marca valida
La marca è in formato TST
La firma della marca è integra

✓ Dettagli marca temporale
Marca temporale emessa in data 13/05/2020 13:54:31 GMT

✓ Il certificato è attendibile
Data-ora di firma attestati dalla marca temporale: 2020-05-13 15:54
Validazione certificato eseguita tramite OCSP

CHIUDI

Se la verifica ha esito positivo si visualizza una spunta verde in corrispondenza di tutti i campi. Nel caso in cui si riscontrino una o più anomalie, ad esempio per Certificato scaduto o non attendibile, il sistema indica il messaggio di errore "Marca KO", attestante che sono stati portati a termine tutti i controlli previsti per la verifica della validità della Firma apposta, ma qualcuno non è andato a buon fine.

L'orario di marcatura e Firma Digitale si riferisce all'orario UTC (Tempo Coordinato Universale) riferimento da cui sono calcolati tutti gli altri fusi orari del mondo e indicato per essere sempre lo stesso in ogni parte del mondo. In Italia, nel periodo estivo (ora "legale"), l'orario è 2 ore avanti rispetto alla UTC (Tempo Coordinato Universale), in inverno (ora "solare") l'orario è avanti di un'ora sulla UTC.

3.12 Generare PIN OTP con Dispositivi di Firma Remota

Generare una password OTP con OTP Display

Per generare un PIN con il dispositivo **OTP con Display**, tenere premuto il **pulsante rosso del proprio dispositivo**, rilasciarlo e attendere che il **codice sia visualizzato sul display**, come da immagine esemplificativa sottostante



Nel caso in cui si utilizzi un dispositivo OTP a evento, cioè un Display c100, (con seriale che inizia per uno), generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, **il Certificato di Firma Remota va fuori sincronizzazione e la procedura di Firma di un documento non va a buon fine. Per ovviare il problema e sbloccare il dispositivo, effettuare la sincronizzazione della Firma.**

38

Generare una password OTP con OTP USB

Per generare un PIN con il dispositivo **OTP USB** inserire il Token in una porta USB. Attendere l'installazione dei driver del dispositivo che risulta conclusa nel momento **in cui si illumina il led al centro del Token stesso**, come da immagine esemplificativa sottostante:



A questo punto eseguire contemporaneamente le operazioni sotto indicate:

- Posizionare il cursore del mouse sopra il riquadro Password OTP
- Sforare con il dito il led luminoso del Token OTP USB collegato alla presa USB del pc

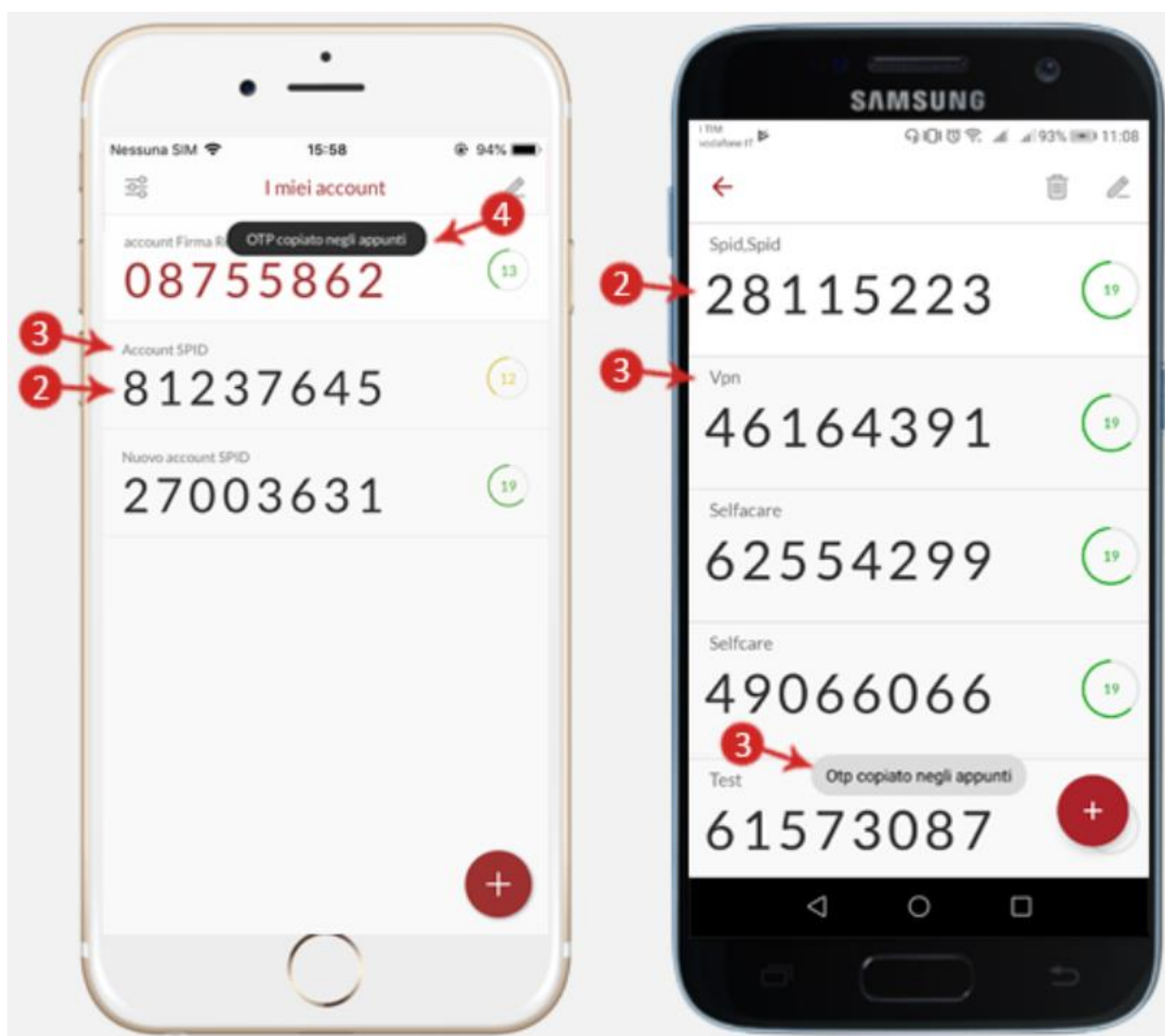
Generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, **il Certificato di Firma**

Remota va fuori sincronizzazione e la procedura di Firma di un documento non va a buon fine. Per ovviare il problema e sbloccare il dispositivo, effettuare la sincronizzazione della Firma.

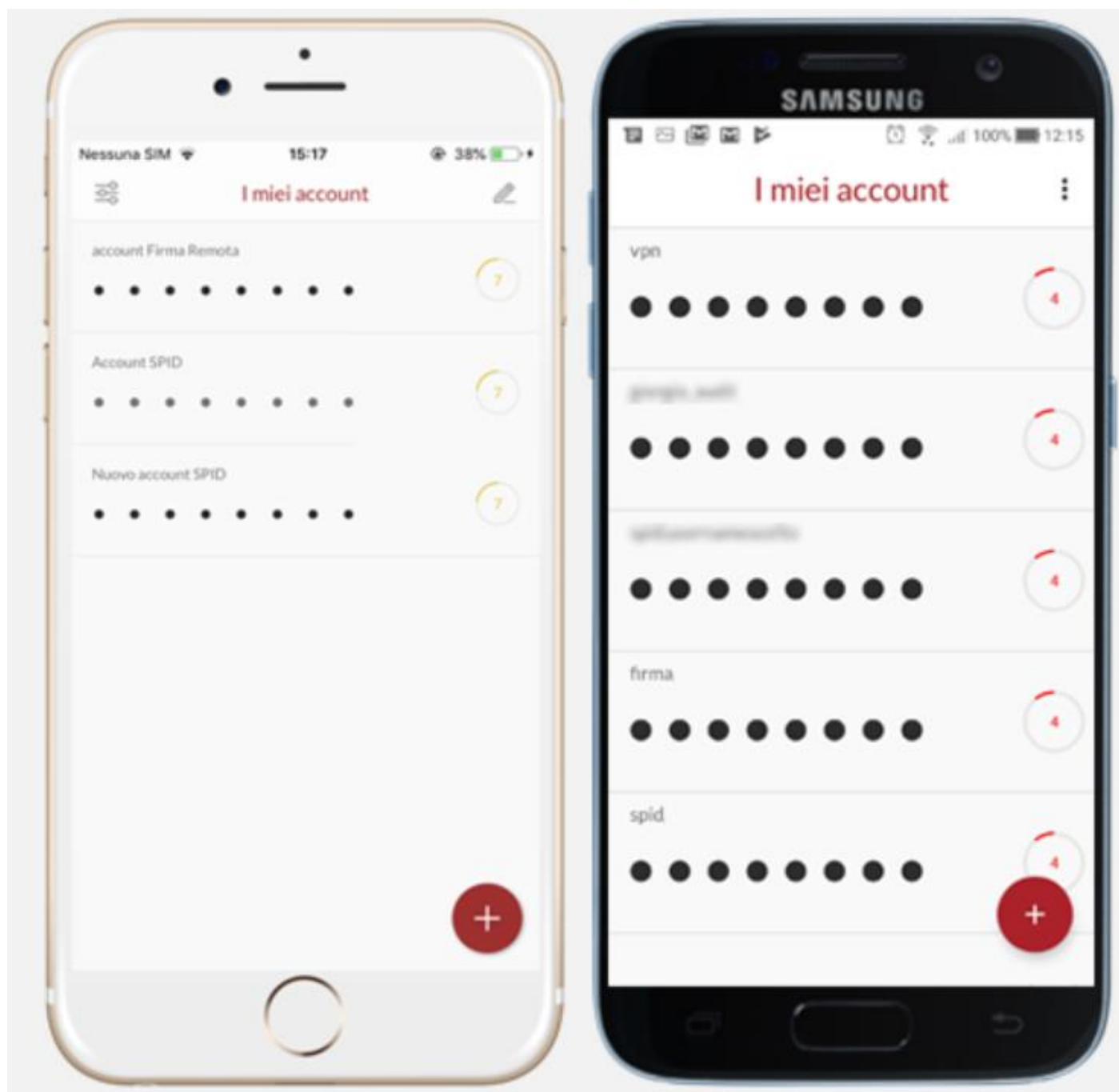
Generare una password OTP con OTP Mobile

L'App **Aruba OTP** genera in automatico **PIN OTP**. Per visionarli:

- 1) Accedere alla App;
- 2) **I PIN OTP generati sono immediatamente visibili** una volta eseguito l'accesso all'applicazione;
- 3) Sopra il Codice è indicato il nome dell'account di riferimento;
- 4) Cliccando sul codice è possibile copiarlo negli appunti:



Nel caso in cui su "Impostazioni" si sia attivata l'opzione "Nascondi OTP", i codici generati non saranno visibili, ma sarà possibile ugualmente copiarli negli appunti:



40

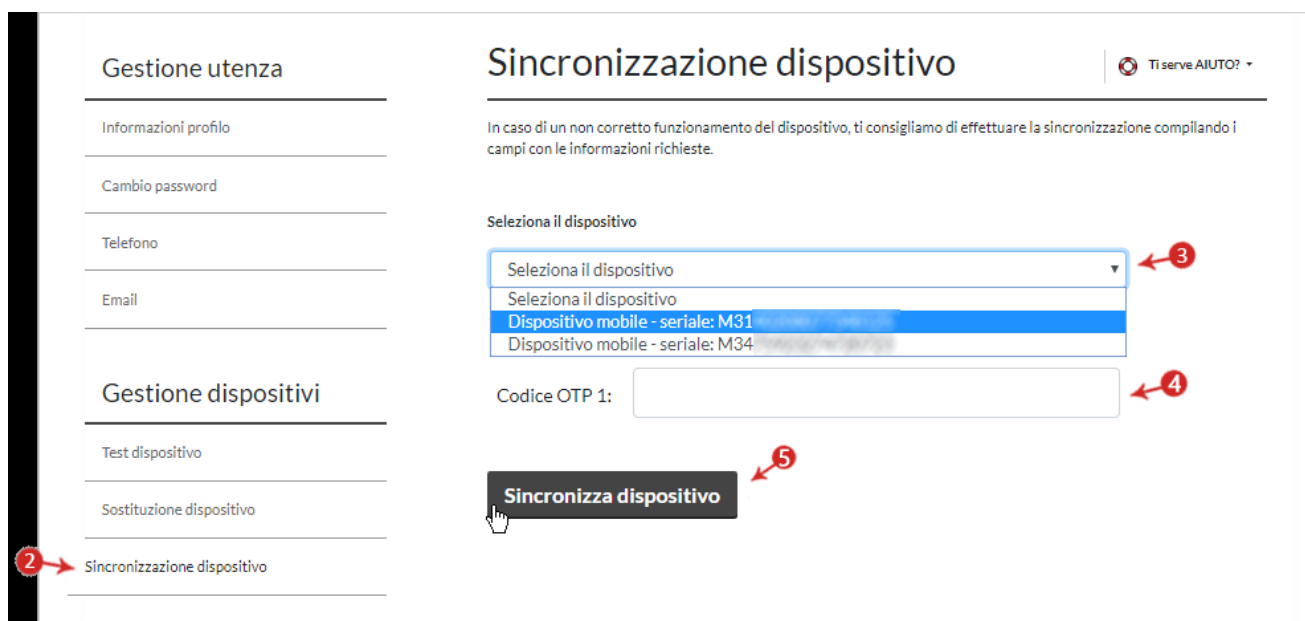
Nel caso in cui si utilizzi **la versione della App OTP mobile precedente a settembre 2016**, generare PIN OTP solo ed esclusivamente in caso di effettivo utilizzo degli stessi per apporre Firma Remota a documenti. Infatti, qualora si generi tramite il proprio Token un tot numero di PIN OTP senza utilizzarli, **il Certificato di Firma Remota va fuori sincronizzazione e la procedura di Firma** di un documento non va a buon fine. **Per ovviare il problema e sbloccare il dispositivo**, effettuare la sincronizzazione della Firma.

4 Sincronizzazione Dispositivo Firma Remota

Qualora si generi con un dispositivo di Firma Digitale Remota (fisico o mobile) un certo numero di PIN OTP senza utilizzarli, o in caso di mal funzionamento del token, il **Certificato di Firma va fuori sincronizzazione** e nonostante l'inserimento di PIN OTP corretti, si visualizza una schermata di errore al termine della Firma di un documento.

Per sbloccare il dispositivo, **sincronizzare la Firma** seguendo la procedura di seguito indicata:

- 1) Accedere al Pannello di Gestione Firma Digitale Remota;
- 2) Dal menu di sinistra selezionare la specifica voce "**Gestione Dispositivi > Sincronizzazione dispositivo**";
- 3) Al Form "**Sincronizzazione dispositivo**" selezionare il dispositivo da sincronizzare dall'apposito menu a tendina;
- 4) Digitare dei codici OTP generati con il dispositivo da sincronizzare:
 - In caso di **Dispositivo OTP a tempo**: OTP con Display c200, cioè con seriale che inizia per due, producono pin temporali che hanno validità 30 o 60 secondi;
 - Per **Dispositivi OTP a evento**: OTP con Display c100, cioè con seriale che inizia per uno e Token OTP USB, producono One Time Password non ripetibili.
- 5) Spuntare su "**Sincronizza dispositivo**" per completare la procedura:



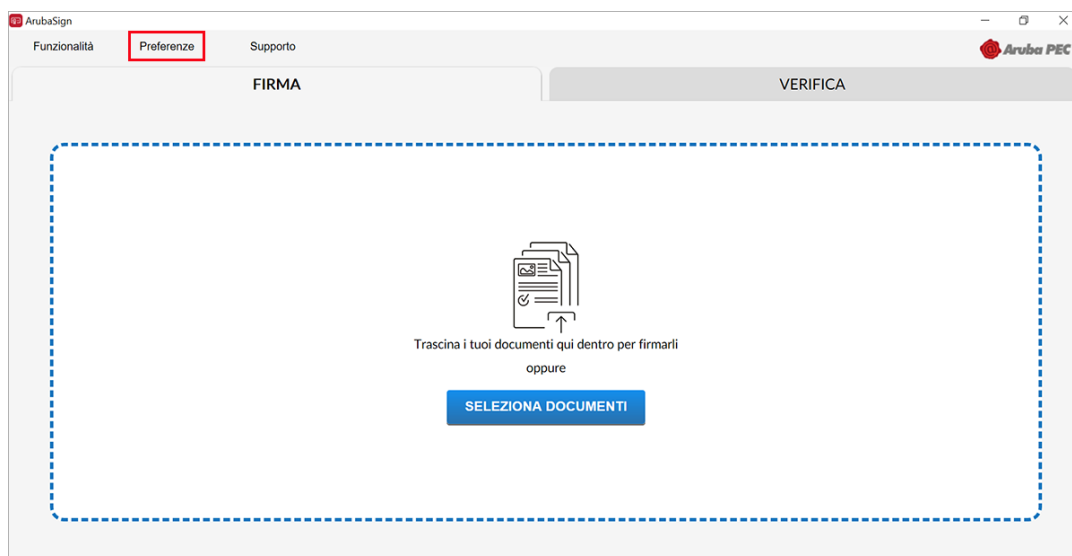
Si visualizza una schermata di conferma.

Qualora la procedura non vada a buon fine e si visualizzi una schermata di errore, aprire una "Richiesta di assistenza" dal portale assistenza.aruba.it, allegando:

- Screenshot dell'errore visualizzato;
- Recapito telefonico e orario di reperibilità (orario di ufficio).

5 Configurazione Proxy http (Firma Remota)

La Configurazione dei Parametri "**Proxy HTTP**", tramite l'utilizzo del **Software Aruba Sign**, permette di svolgere le operazioni di verifica di un file firmato, aggiornamento, controllo, stato di revoca e richiesta di Marche Temporalì qualora la postazione si trovi dietro Proxy HTTP. Per procedere, aprire il menu "**Preferenze**" di Aruba Sign:



Quindi allo specifico Tab "**Proxy**" è possibile scegliere:

- Nessun Proxy
- Configurazione Manuale
- Configurazione di sistema

42

Se si sceglie la Configurazione manuale impostare i relativi parametri e salvarli. Di seguito un esempio di configurazione:

Proxy generico
<input type="radio"/> Nessun proxy
<input checked="" type="radio"/> Configurazione manuale
<input type="radio"/> Configurazione di sistema
Tipo
<input checked="" type="radio"/> HTTP
<input type="radio"/> SOCKS4
<input type="radio"/> SOCKS5
<input type="radio"/> NTLM

Proxy Url: 192.168.1.1

Proxy Port: 8080

Proxy User: Nome utente

Proxy Password: Password

Cliccare su "**Salva**" per completare l'operazione.

Qualora non siano disponibili i dati relativi a una delle due sezioni HTTP o LDAP ad esempio nel caso in cui la rete non supporti entrambe le configurazioni, procedere solo con la creazione relativa alla tipologia di Proxy supportata.

6 Installazione e avvio del Software – Firma Digitale

I Kit di Firma Digitale Aruba sono composti da **Token o lettori da tavolo**, **Smart Card** (in formato SIM e carta di credito) e **certificato di Firma e Autenticazione CNS**.

In caso di acquisto del Kit completo, prima di scaricare il Software Aruba Sign, installare i driver necessari al riconoscimento del lettore e della Smart Card acquistati. In caso di acquisto di una Smart Card, installare i soli driver relativi.

6.1 Installare i driver dei Lettori di Firma Digitale

Collegare il Lettore al PC e attendere il riconoscimento del sistema, quindi inserire la carta nel lettore con il chip rivolto verso l'alto:



43

Dalla sezione “Download Software e Driver” del sito pec.it, al Form dedicato **Driver Lettori** cliccare su **Scarica il Software** a seconda del sistema operativo utilizzato (l'immagine esemplificativa di seguito indicata si riferisce a **Windows**):

DRIVER LETTORI

- Lettori

Il lettore è il dispositivo fisico in cui inserire la Card di Firma e che, una volta collegato al computer, consente l'utilizzo del servizio.
Per poterlo utilizzare è necessario installare i driver del lettore nel tuo computer.

Per installare i driver del lettore dovrai:

- Scaricare e salvare i relativi driver in base al sistema operativo presente sul tuo computer;
- Decomprimere ed eseguire il file .exe;
- Completare la procedura di installazione.

Windows

Scarica il Software

Apple

Scarica il Software

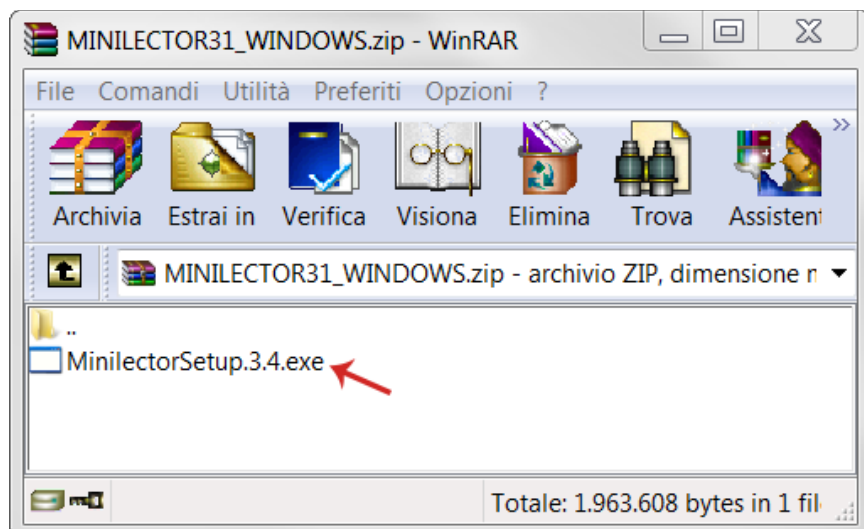
Linux

Scarica il Software

Utilizzabile con:



Dalla cartella creata a seguito dell'installazione, decomprimere ed eseguire il file .exe, quindi completare la procedura di installazione, seguendo i passaggi indicati dal sistema:



6.2 Installare i driver Smart Card

- 1) Confrontare l'immagine del chip della carta posseduta con quelle indicate nelle sezioni dedicate del sito pec.it, visionabili dall'apposito menu a tendina al link <https://www.pec.it/download-software-driver.aspx>;
- 2) Scaricare e salvare i relativi driver cliccando sul pulsante Scarica il Software in base al sistema operativo presente sul proprio computer (l'immagine esemplificativa di seguito indicata si riferisce a Chip Incard o Obertur e sistema operativo Windows):

44

DRIVER SMART/SIM CARD

- CARD produttore Incard e Oberthur

Per poter utilizzare il servizio di Firma è necessario innanzi tutto installare i driver delle Card nel tuo computer.
Confronta le immagini del chip con quella della tua Card e procedi con il download del software.

Per installare i driver della Card dovrai:

- Scaricare e salvare i relativi driver in base al sistema operativo presente sul tuo computer;
- Decomprimere ed eseguire il file .exe;
- Completare la procedura di installazione.

Utilizzabile con:

Chip Incard

Chip Oberthur

Windows

Apple

Linux

Scarica il Software

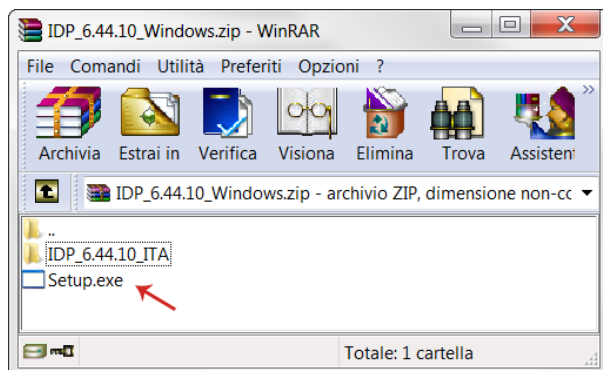
Scarica il Software

Scarica il Software

Se l'immagine sul tuo chip non corrisponde ad una di quelle qui indicate, seleziona CARD produttore Athena.

+ CARD produttore Athena

- 3) Dalla cartella creata a seguito dell'installazione, decomprimere ed eseguire il file .exe, quindi completare la procedura di installazione, seguendo i passaggi indicati dal sistema:



6.3 Installare il software Aruba Sign

- 1) Collegarsi a <https://www.pec.it/download-software-driver.aspx>;
- 2) Dal menu a tendina **Software** → selezionare **Software di Firma Aruba Sign**, quindi cliccare sul pulsante **Scarica il Software corrispondente al sistema operativo utilizzato** (l'esempio di seguito indicato si riferisce a Windows):

SOFTWARE

Software di firma ArubaSign

Aruba Sign è il software che consente di apporre, gestire e verificare firme digitali e marche temporali. Dopo aver installato i driver della Card e/o del lettore, è necessario installare il software Aruba Sign sul tuo computer per la gestione del servizio di Firma.

N.B.: se disponi di «Aruba Key» non dovrai scaricare alcun software perché già installato nel tuo dispositivo.

Per installare Aruba Sign dovrai:

- Scaricare e salvare il file di installazione in base al sistema operativo presente sul tuo computer;
- Eseguire il file .exe;
- Completare la procedura di installazione.

Windows Apple Linux 64bit Linux 32bit

Scarica il Software Scarica il Software Scarica il Software Scarica il Software

Windows (ipovedenti)

Scarica il Software

Utilizzabile con:

Token Smart Card OTP display OTP USB OTP Mobile

+ Software per ArubaKey

+ Software rinnovo

- 3) **Scaricare ed eseguire su locale il File di installazione**, quindi installare il Software utilizzando la procedura guidata:
 - selezionare la Lingua di Installazione;

- installazione di Aruba Sign, cliccare su Avanti;
 - selezionare la cartella di destinazione e cliccare su Avanti;
 - premere Installa per continuare l'installazione;
 - attendere il completamento dell'installazione di Aruba Sign sul computer;
 - premere Fine per completare l'installazione.
- 4) Completo il processo, **sul desktop si visualizza l'icona di Aruba Sign** che permette l'avvio del programma.
- 5) Completata l'installazione, si visualizza la schermata principale del Software:



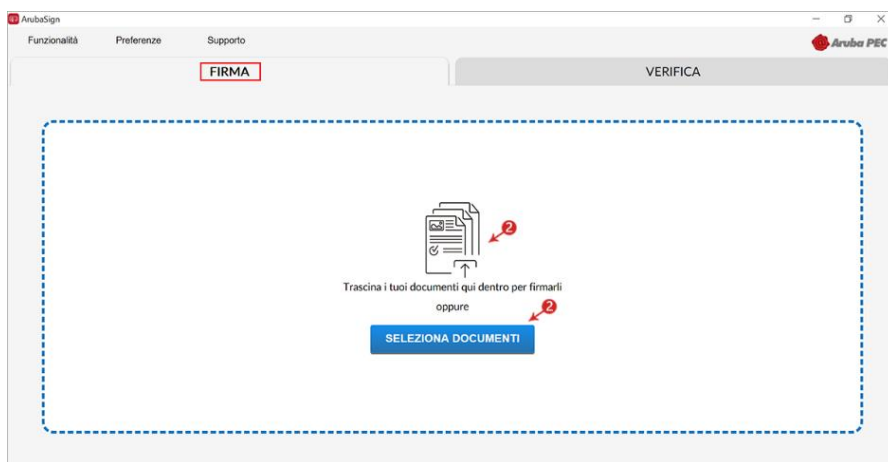
46

7 Firma e verifica file Aruba Sign - Firma Digitale

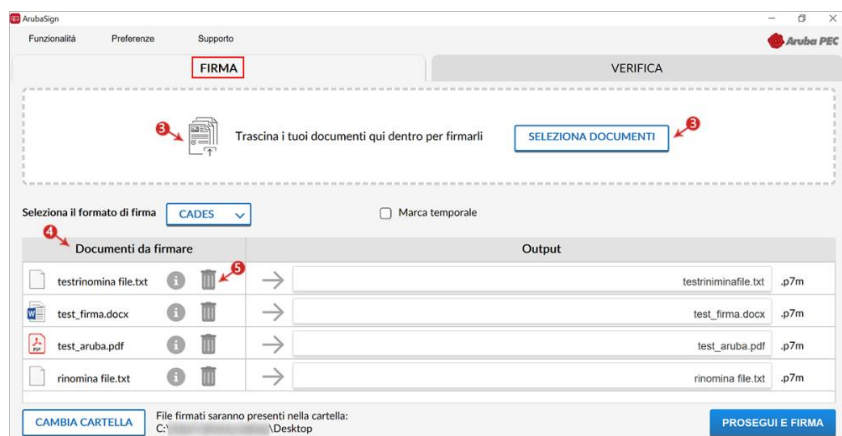
7.1 Caricamento documenti da firmare e/o cartelle su Aruba Sign

Per caricare uno o più file su Aruba Sign e/o una intera cartella:

- 1) aprire il Software Aruba Sign;
- 2) nella scheda **FIRMA** è possibile trascinare un qualsiasi documento e/o cartella o selezionare un documento da **SELEZIONA DOCUMENTI** (sono accettate tutte le estensioni):



- 3) per aggiungere ulteriori documenti, cliccare su **SELEZIONA DOCUMENTI** e caricare i file desiderati da locale o trascinare il file. Gli stessi sono visibili in elenco su **Documenti da firmare**;
- 4) sono visibili i documenti importati in corrispondenza di **Documenti da firmare**;
- 5) i documenti caricati possono essere rimossi in qualsiasi momento cliccando sull'icona **Cestino**:



7.2 Firma uno o più file in formato .p7m - Firma Digitale

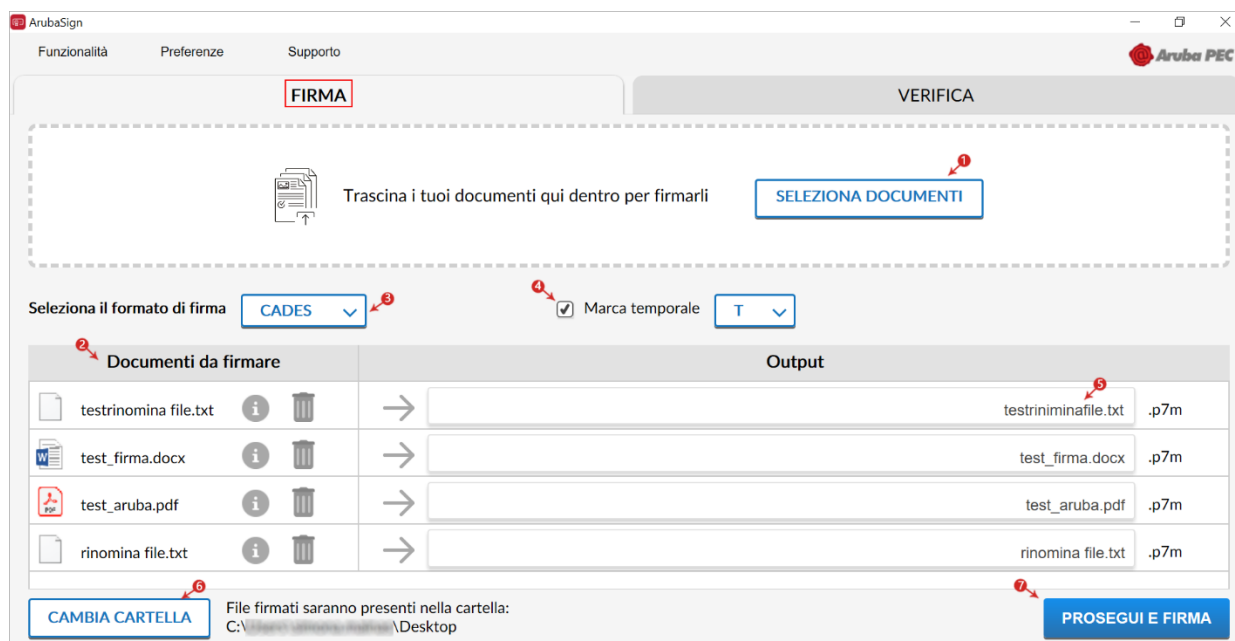
Un **file firmato digitalmente** assume estensione **.p7m**, che si somma all'estensione del file originario. Ad esempio, un **documento .txt**, al **termine del processo di Firma Digitale** diviene un **documento .txt.p7m** che rappresenta una **busta informatica (PKCS#7)**. La busta incorpora al suo interno il documento originario, il certificato del sottoscrittore e un hash del documento firmato con il certificato del sottoscrittore. Un documento sottoscritto digitalmente ha piena validità legale.

47

Per **firmare digitalmente uno o più file in formato .p7m (Firma CADES)** e/o una intera cartella **con Aruba Sign**:

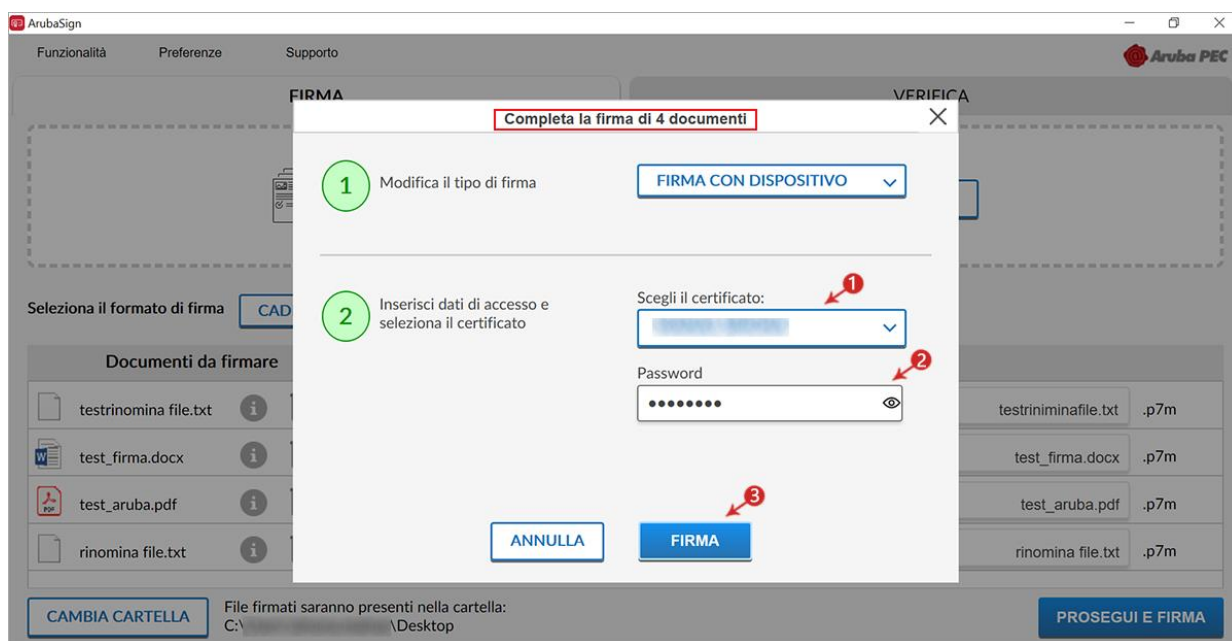
- 1) trascinare o selezionare uno o più documenti e/o una intera cartella;
- 2) il **singolo/i documenti caricati/o** sono visibili all'apposita schermata **Documenti da firmare**;
- 3) dall'apposito menu a tendina **Seleziona il formato firma** selezionare come tipologia di firma **CADES** per firmare il file in formato .p7m;
- 4) se in possesso di Marche Temporal, oltre alla firma, è possibile apporre al file una marcatura temporale. Inserire il flag in corrispondenza della voce **Marca Temporale** nel formato scelto dall'apposito menu a tendina;
- 5) dalla finestra **Output** rinominare, se desiderato, eventuali file prima di apporre la firma;
- 6) da **CAMBIA CARTELLA** verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;

cliccare su **PROSEGUI E FIRMA** per continuare. Sono firmati tutti i documenti presenti alla finestra **Documenti da firmare**:



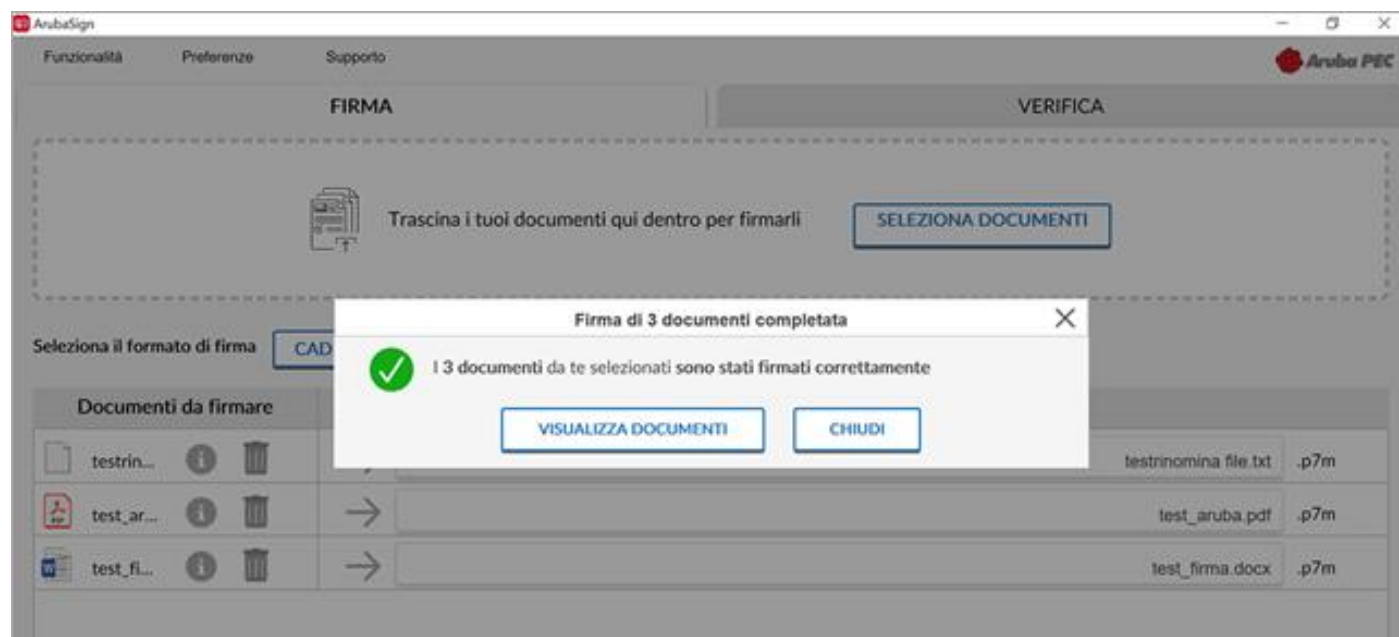
Alla schermata **Completa la firma di 4 documenti**:

- 1) assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);
- 2) inserire il **PIN** di protezione della **Smart Card**;
- 3) cliccare su **FIRMA** per concludere il processo:



Al termine dell'operazione si visualizza la corretta firma del file.

Su **VISUALIZZA DOCUMENTI** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **CHIUDI** per terminare l'operazione:



7.3 Firma un singolo file in formato ASiC-S - Firma Digitale

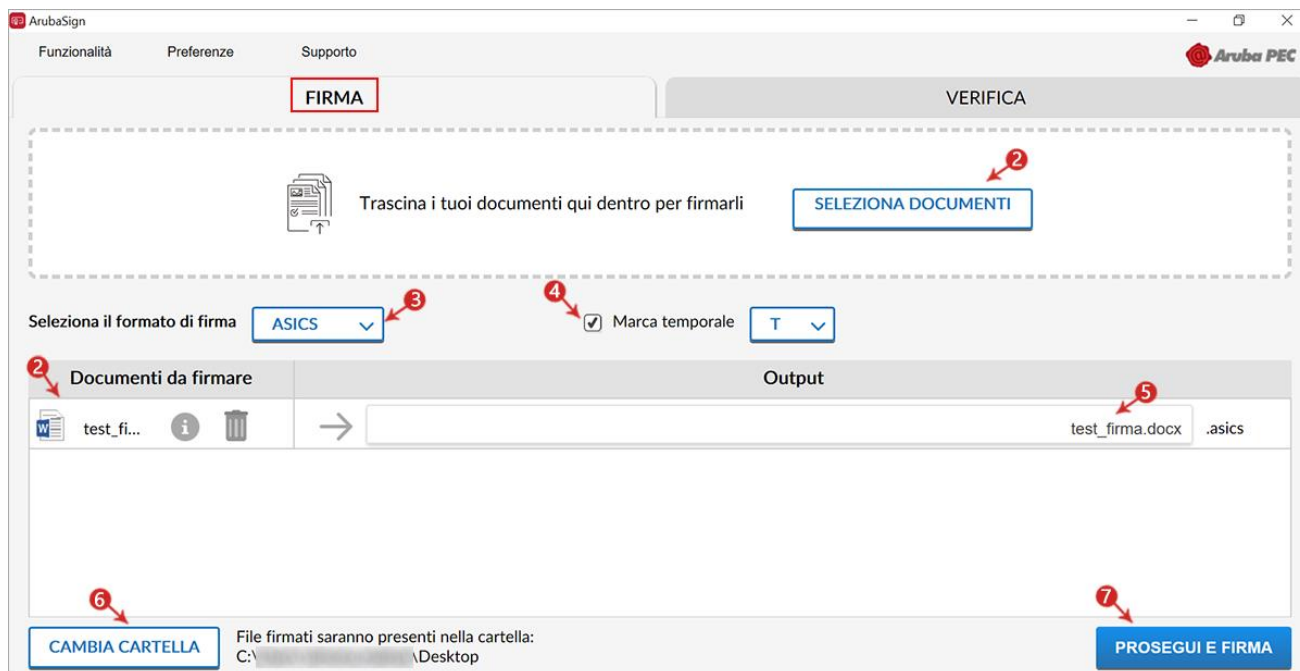
Il formato di firma **asic-s** (**Associated Signature Containers ASiC simple**) è un **contenitore di dati che raggruppa un file e le relative firme digitali detached e/o marche temporali associate**, utilizzando il formato **.zip**.

49

Per **firmare digitalmente un file in formato ASiC-S con Aruba Sign**:

- 1) **caricare il documento**. Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di un singolo File.
- 2) I **singolo/i documenti caricati/o** sono visibili all'apposita schermata **Documenti da firmare**;
- 3) dal menu a tendina **Seleziona il formato di firma** selezionare come tipologia di Firma **ASiC-S**;
- 4) se in possesso di Marche Temporali, oltre alla firma, è possibile apporre al file una marcatura temporale;
- 5) dalla finestra **Output** rinominare, se desiderato, il file;
- 6) da **CAMBIA CARTELLA** verificare che il percorso utilizzato per salvare il file firmato sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;

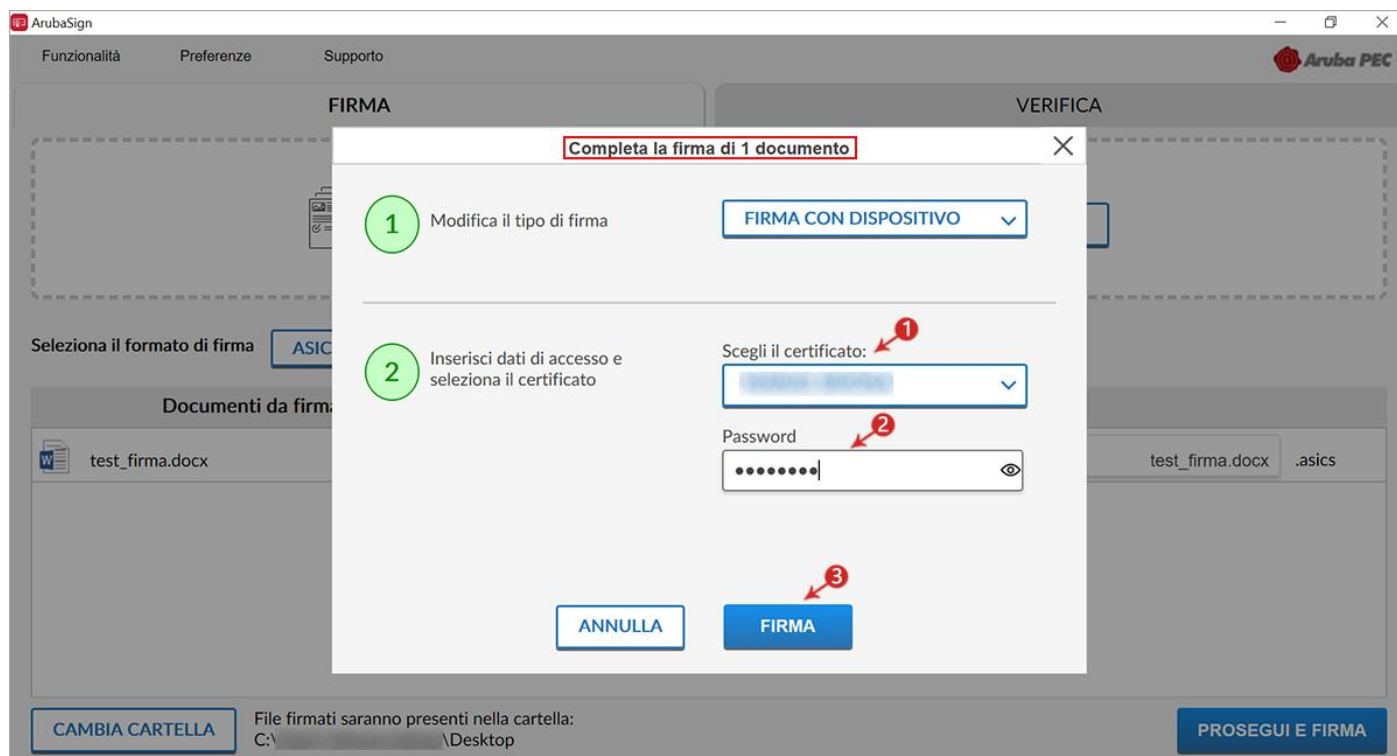
7) cliccare su **PROSEGUI E FIRMA** per continuare:



Alla schermata **Completa la firma di 1 documento**:

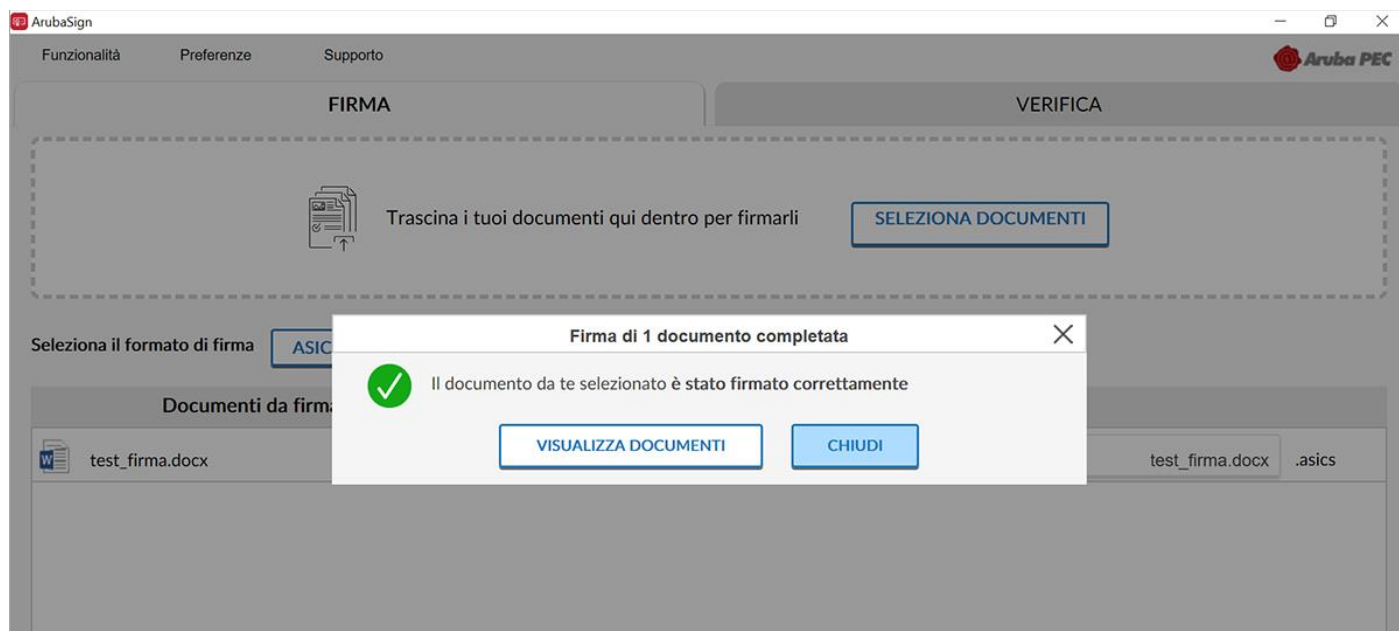
- 1) assicurarsi che sia selezionato il **Certificato per la firma digitale** (in formato Cognome - Nome);
- 2) inserire il **PIN** di protezione della **Smart Card**;
- 3) cliccare su **FIRMA** per concludere il processo:

50



Al termine dell'operazione si visualizza la corretta firma del file.

Su **VISUALIZZA DOCUMENTI** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **CHIUDI** per terminare l'operazione:



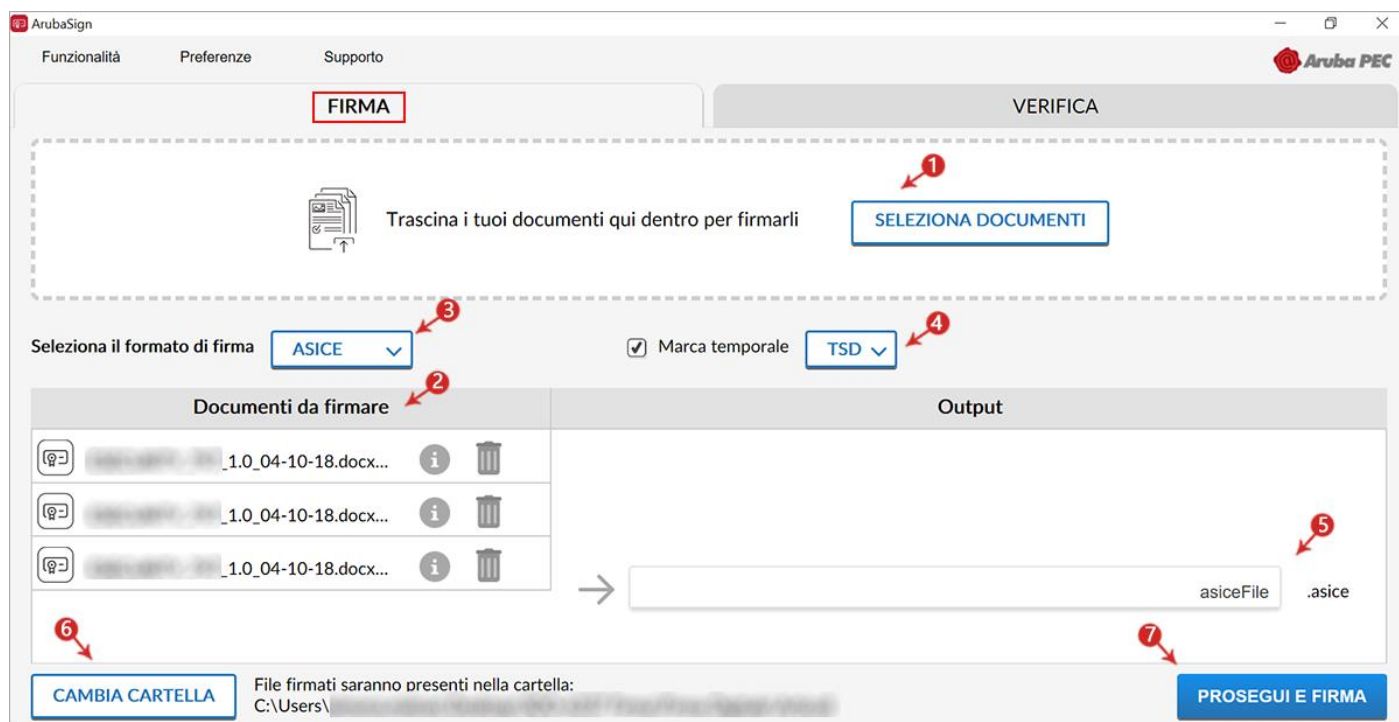
Il documento firmato in formato **ASiC-S** è salvato nella cartella indicata in fase di firma.

7.4 Firma di più file in formato ASiC-E - Firma Digitale

51

Il formato di firma ASiC-E (Associated Signature Containers "ASiC extended") è un contenitore di dati che raggruppa più file e le relative firme digitali detached e/o marche temporali associate, utilizzando il formato .zip. Per **firmare digitalmente più file in formato ASiC-E con Aruba Sign**:

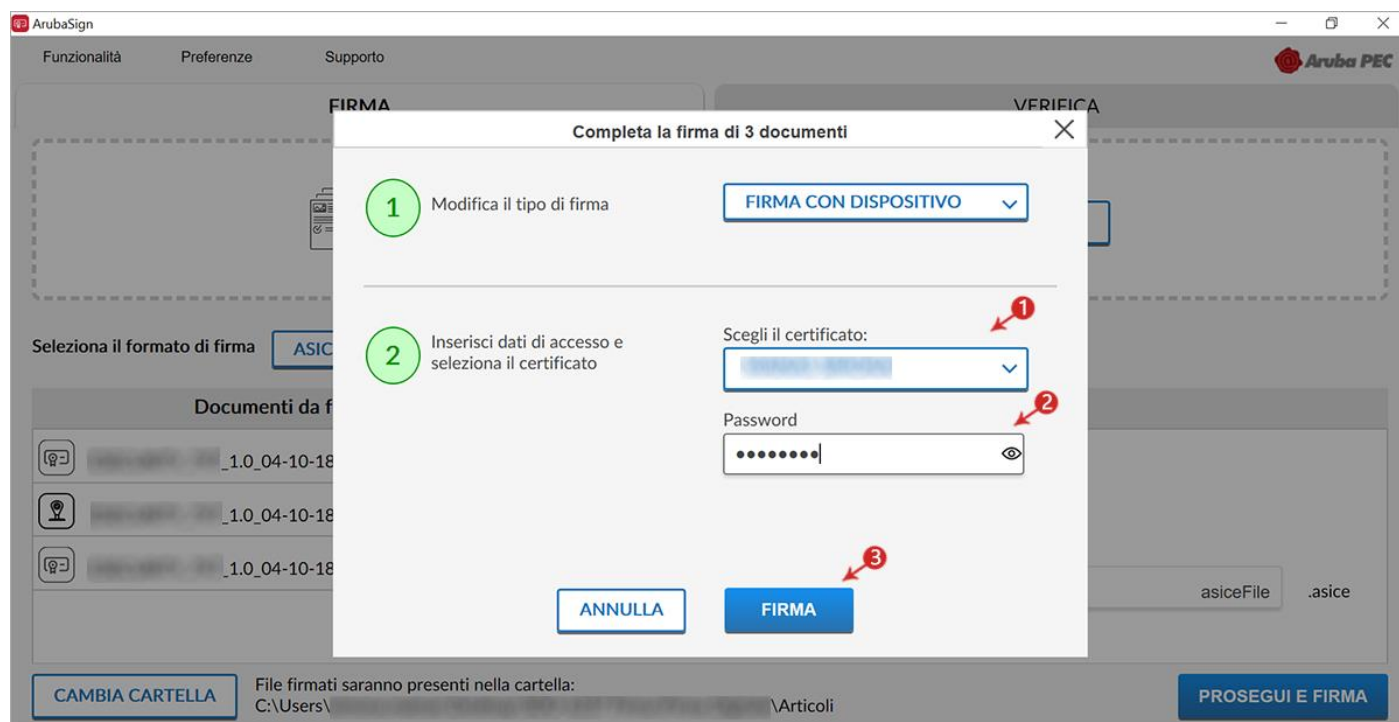
- 1) caricare i documenti e/o una intera cartella. Questo formato di Firma è applicabile solo in caso di caricamento su Aruba Sign di più documenti, per firmare un solo file in formato ASiC,
- 2) i documenti caricati sono visibili all'apposita schermata Documenti da firmare;
- 3) dal menu a tendina Seleziona il formato di firma selezionare come tipologia di Firma ASiC-E;
- 4) se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale;
- 5) dalla finestra Output rinominare, se desiderato, il contenitore dei file;
- 6) da CAMBIA CARTELLA verificare che il percorso utilizzato per salvare i file firmati sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
- 7) cliccare su PROSEGUI E FIRMA per continuare. Sono firmati tutti i documenti presenti alla finestra Documenti da firmare:



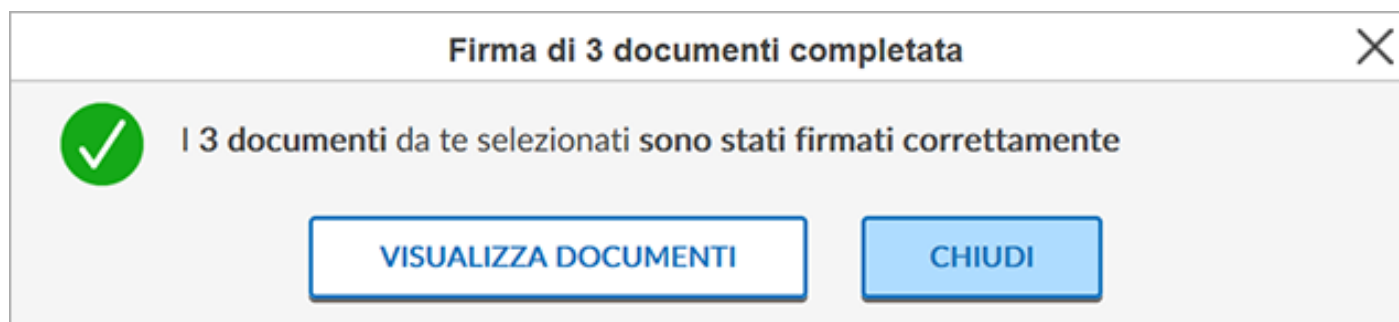
Alla schermata **Completa la firma di 3 documenti**:

- 1) assicurarsi che sia selezionato il Certificato per la firma digitale (in formato Cognome - Nome);
- 2) inserire il **PIN** di protezione della Smart Card;
- 3) cliccare su **FIRMA** per concludere il processo:

52



Su **VISUALIZZA DOCUMENTI** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **CHIUDI** per terminare l'operazione:

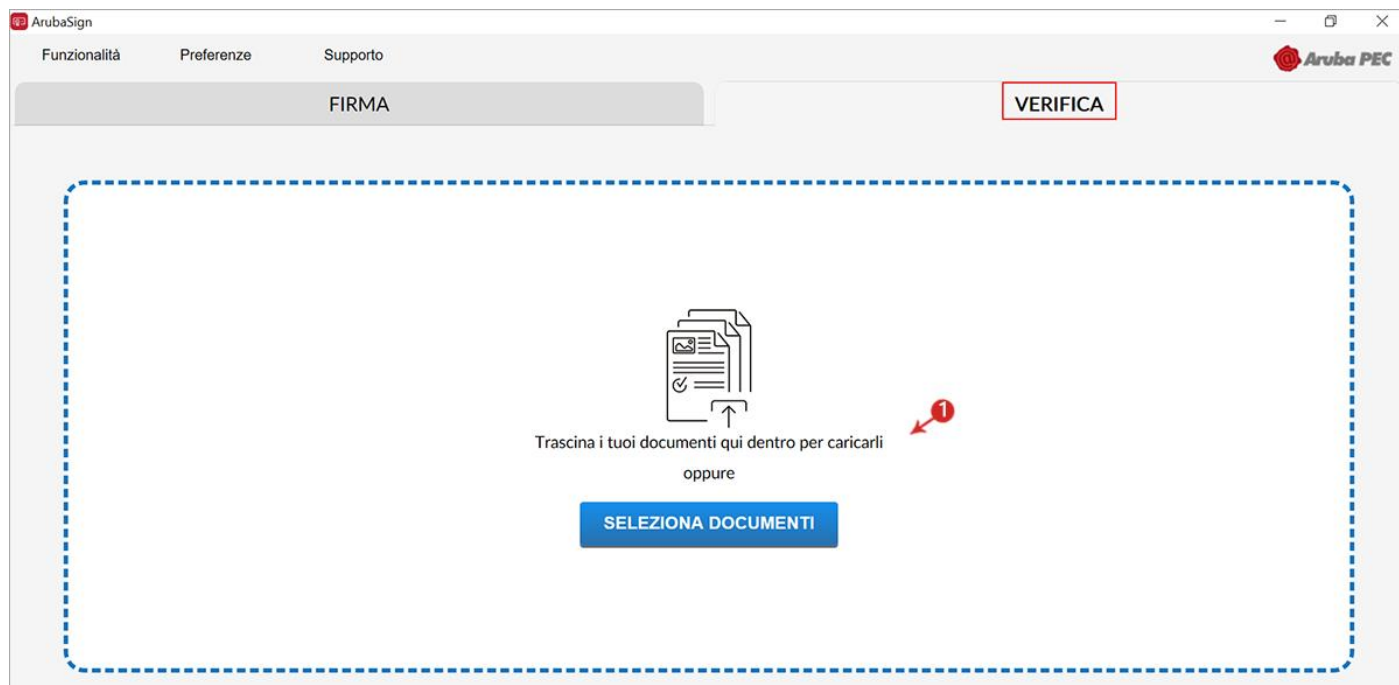


Il contenitore di documenti in formato **ASiC-E** è salvato nella cartella indicata in fase di Firma. In fase di verifica del contenitore è possibile visionare il dettaglio delle firme apposte a ogni singolo documento.

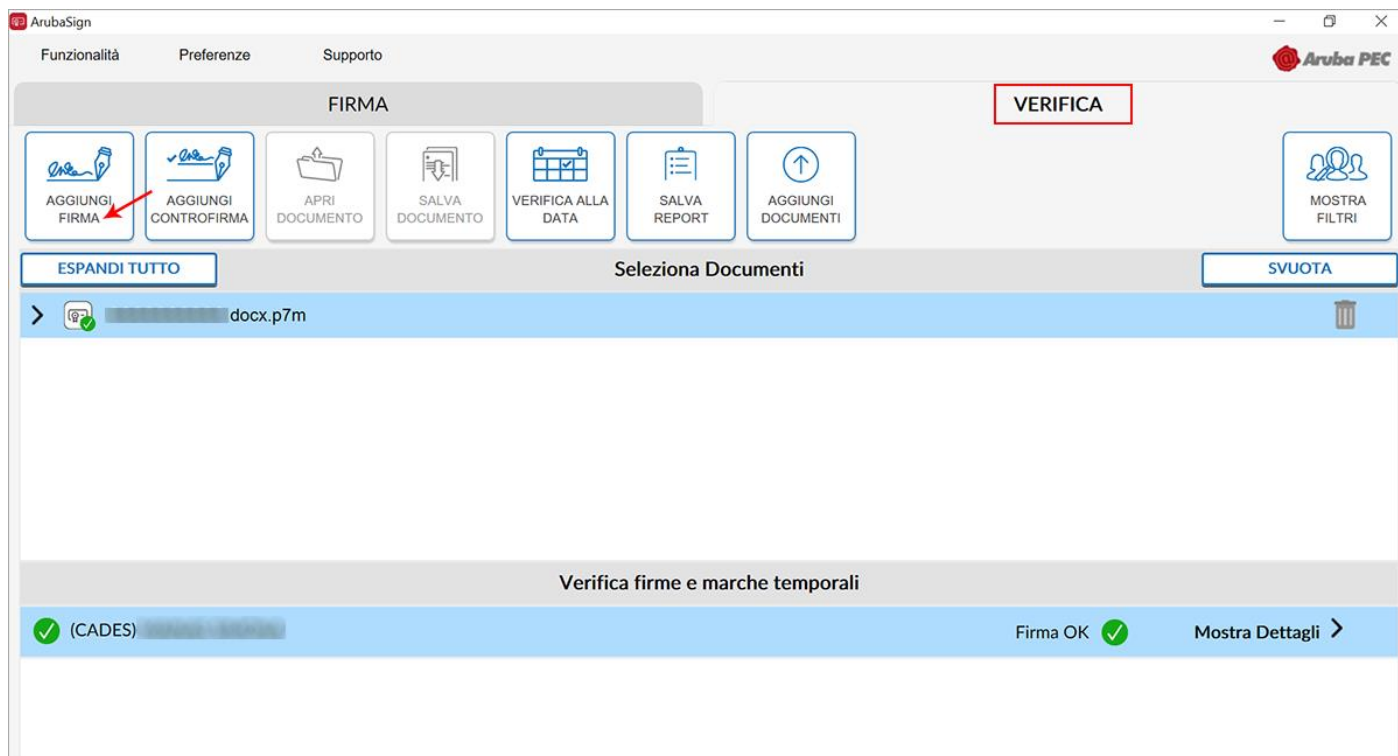
7.5 Apposizione Firma Parallela - Firma Digitale

La funzione **Firma Parallela** è accessibile trascinando o selezionando il documento all'interno della scheda **VERIFICA** del Software Aruba Sign uno o più file già firmati in **formato .p7m (CADES)** o **.PDF (PAdES)**. È aggiunta allo stesso livello e allo stesso contenuto di una firma preesistente e viene di norma utilizzata per aggiungere firme ad un documento già firmato in **formato .p7m** in quei flussi documentali che ne prevedono l'utilizzo.

Per crearla selezionare o trascinare un file .p7m (CADES) o .PDF (PAdES), sopra il menu **VERIFICA** di Aruba Sign:



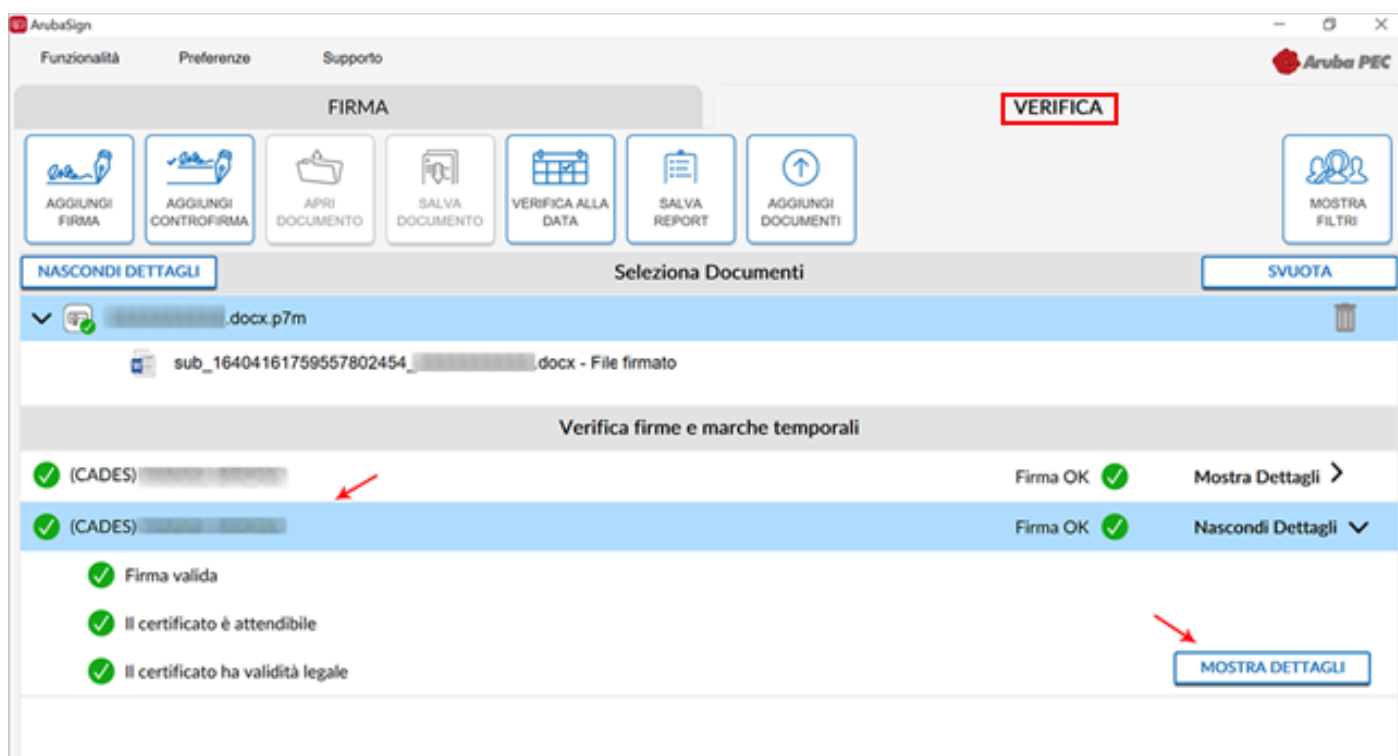
Selezionato il documento (anche in caso di caricamento di un solo file) su cui apporre la **Firma Parallela** poi cliccare su **AGGIUNGI FIRMA**:



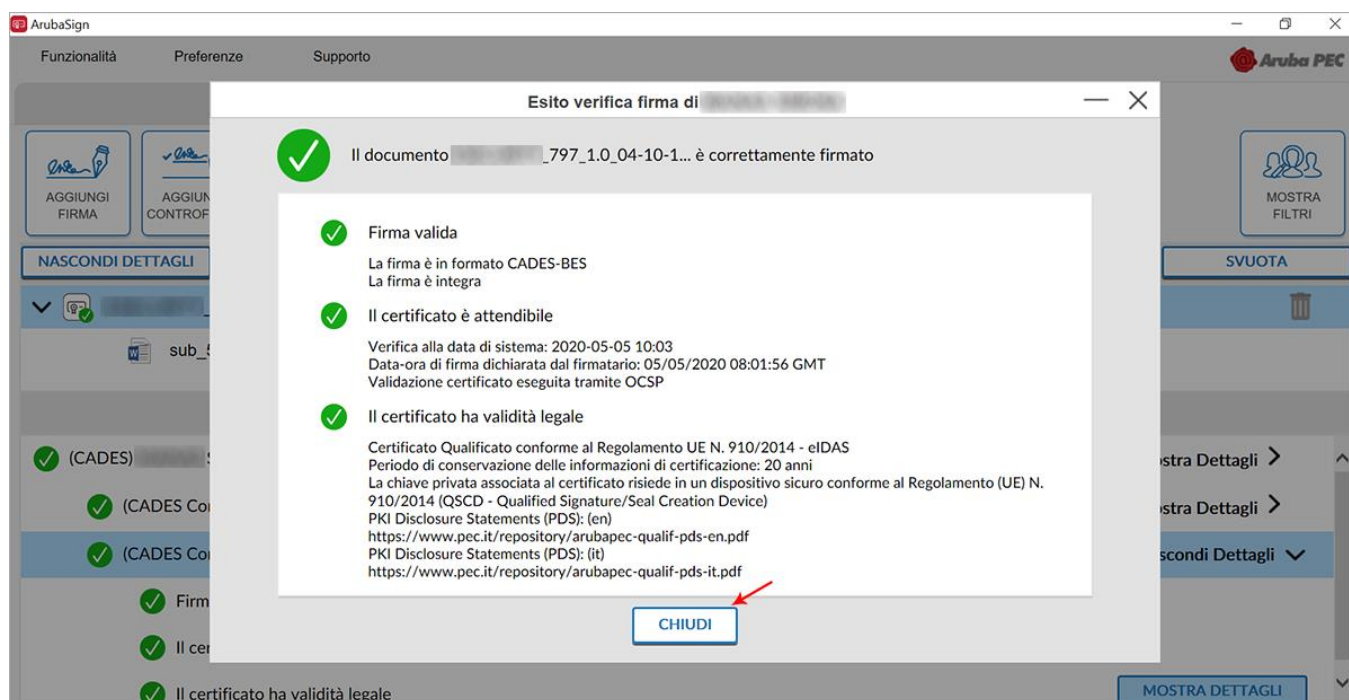
Firmare digitalmente il file. Il sistema non consente di selezionare il formato della Firma. In caso di File .p7m la **Firma Parallela** è apposta in tale formato (per i dettagli della procedura cliccare qui), per i file .PDF è possibile apporre una Firma Grafica o Invisibile. **La nuova firma è apposta allo stesso livello di quella preesistente.**

54

È possibile visionare la presenza della **Firma Parallela** e i dettagli su **MOSTRA DETTAGLI** come da immagine esemplificativa sottostante:



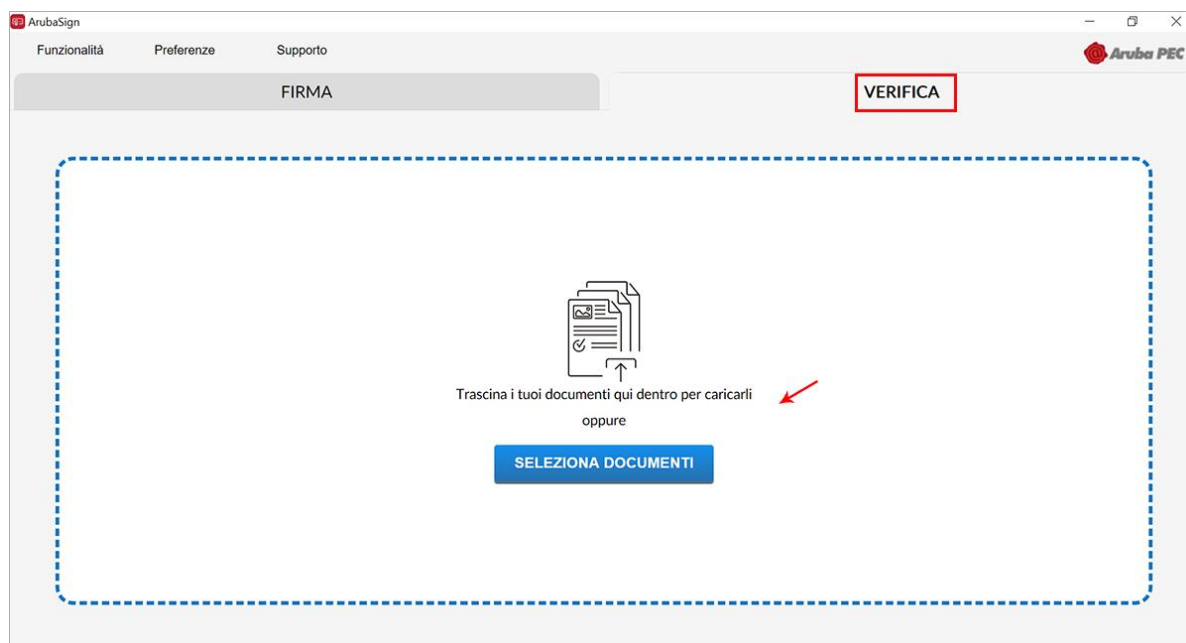
E infine su **MOSTRA DETTAGLI** l'esito di verifica:



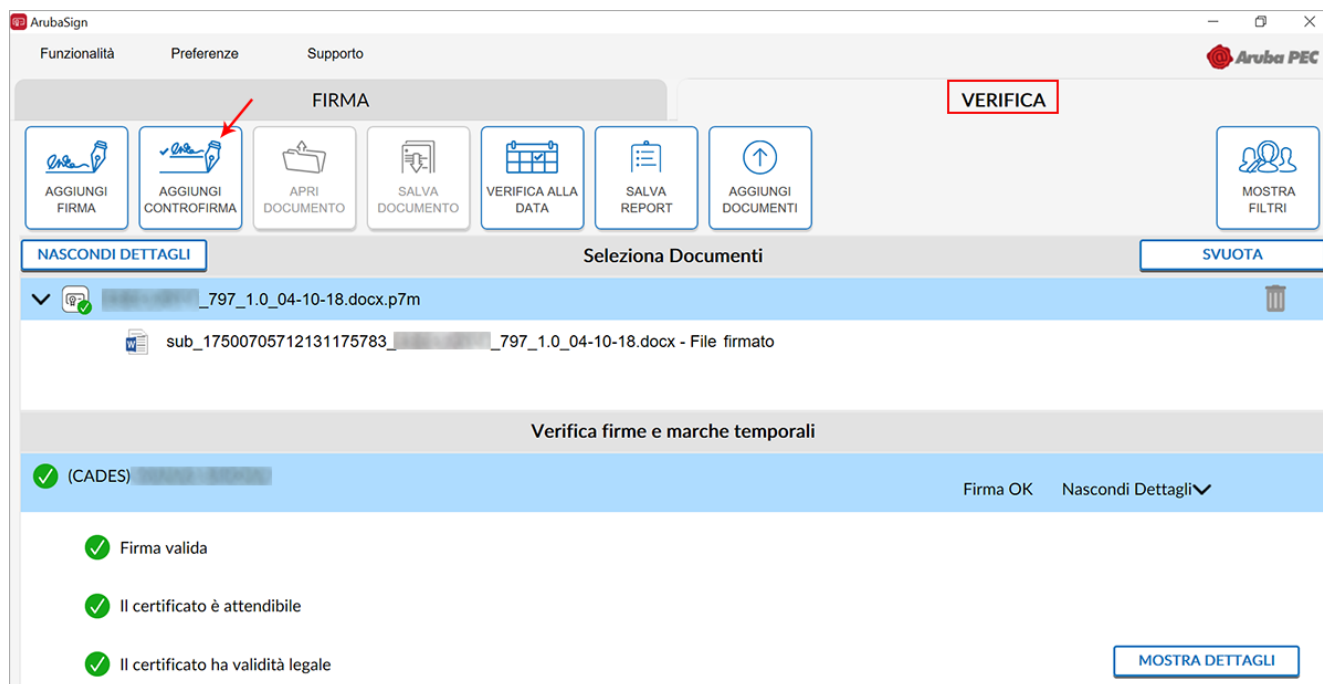
7.6 Apposizione Controfirma - Firma Digitale

La funzione **Controfirma** è accessibile trascinando o selezionando il documento all'interno della scheda **VERIFICA** del Software Aruba Sign **uno o più file già firmati in formato .p7m**. È apposta a un livello sottostante di una firma preesistente e sottoscrive quest'ultima. È più annidata rispetto alla firma a cui si riferisce (aspetto evidenziato da una rappresentazione ad albero delle firme stesse).

Per crearla **selezionare o trascinare un file .p7m (CADES)**, su **VERIFICA** di Aruba Sign:



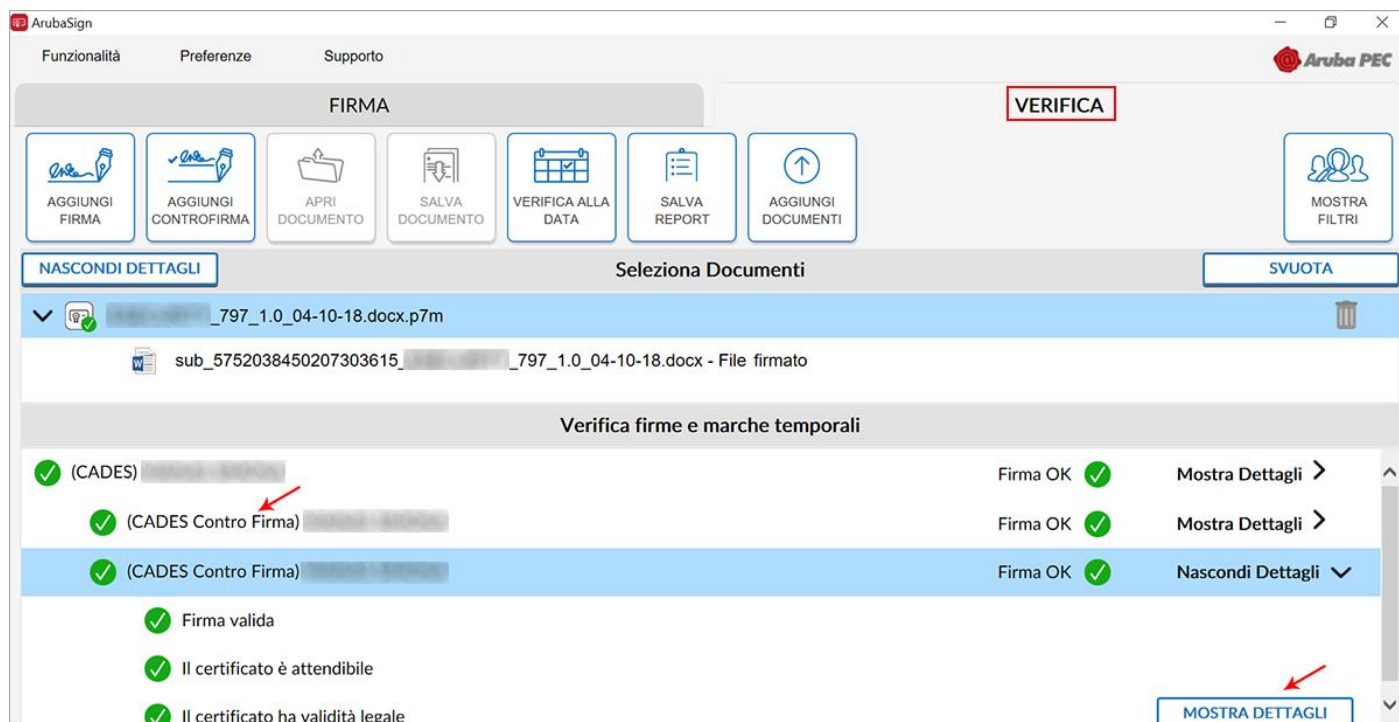
Selezionato il documento (anche in caso di caricamento di un solo file) su cui apporre la Controfirma cliccare su **AGGIUNGI CONTROFIRMA**:



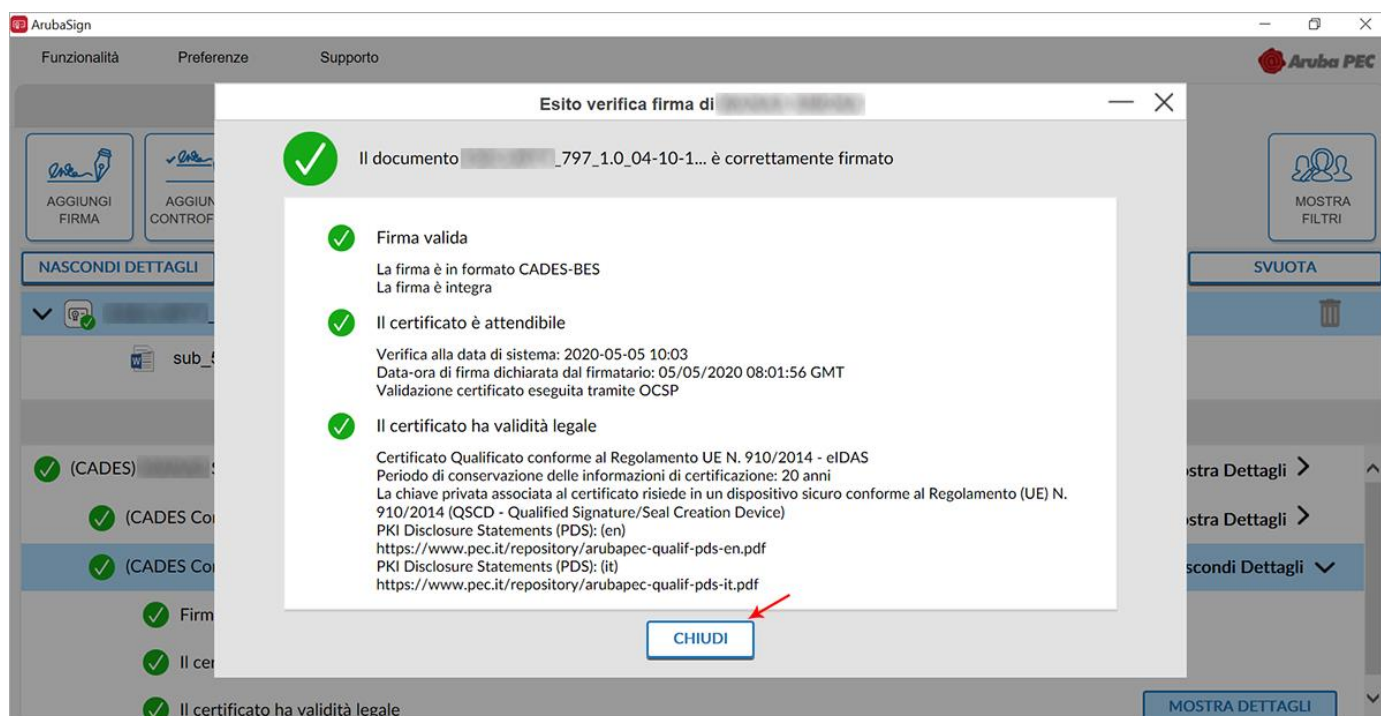
Firmare digitalmente il file in formato .p7m. La nuova firma è apposta a un livello sottostante della firma preesistente.

È possibile visionare la presenza della **Controfirma**, come da immagine esemplificativa sottostante:

56



E infine su **MOSTRA DETTAGLI** l'esito di verifica firma:



7.7 Apposizione Firma PDF – Grafica - Firma Digitale

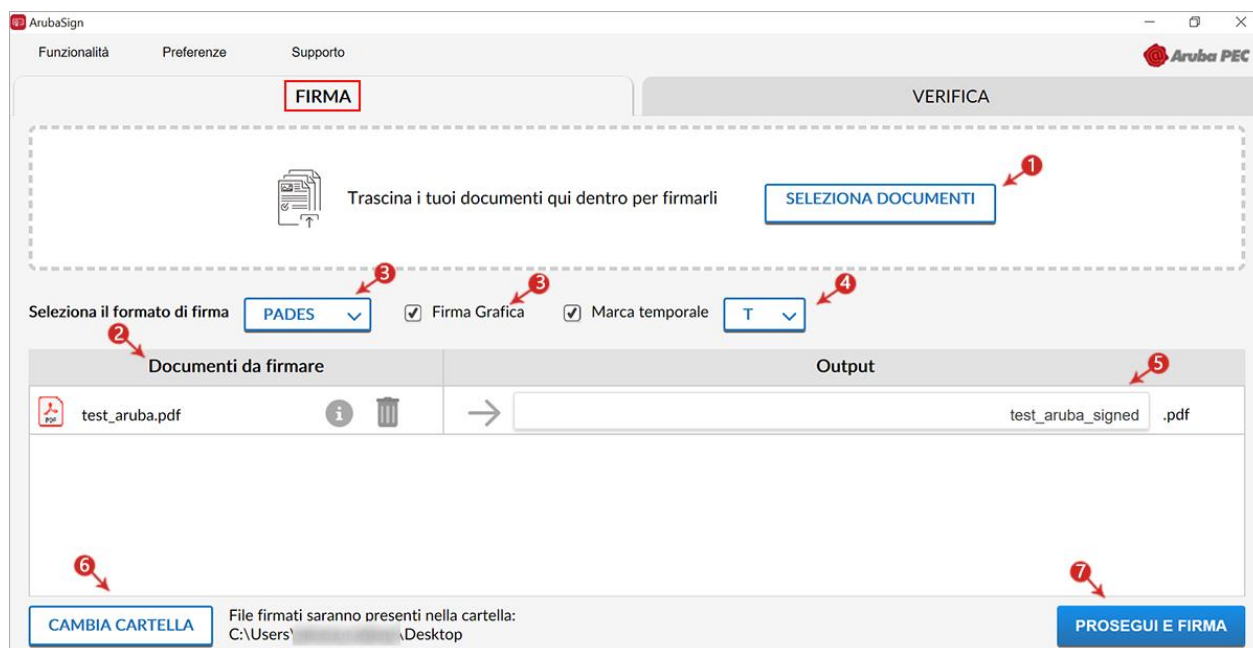
57

Il Formato di Firma **PAdES** è applicabile ai soli file **.PDF, .doc, .docx, .xls, .xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

La Firma PAdES - Firma Grafica permette di scegliere la posizione e la dimensione del campo che ospita la Firma Digitale.

Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Grafica** e/o una intera cartella **con Aruba Sign**:

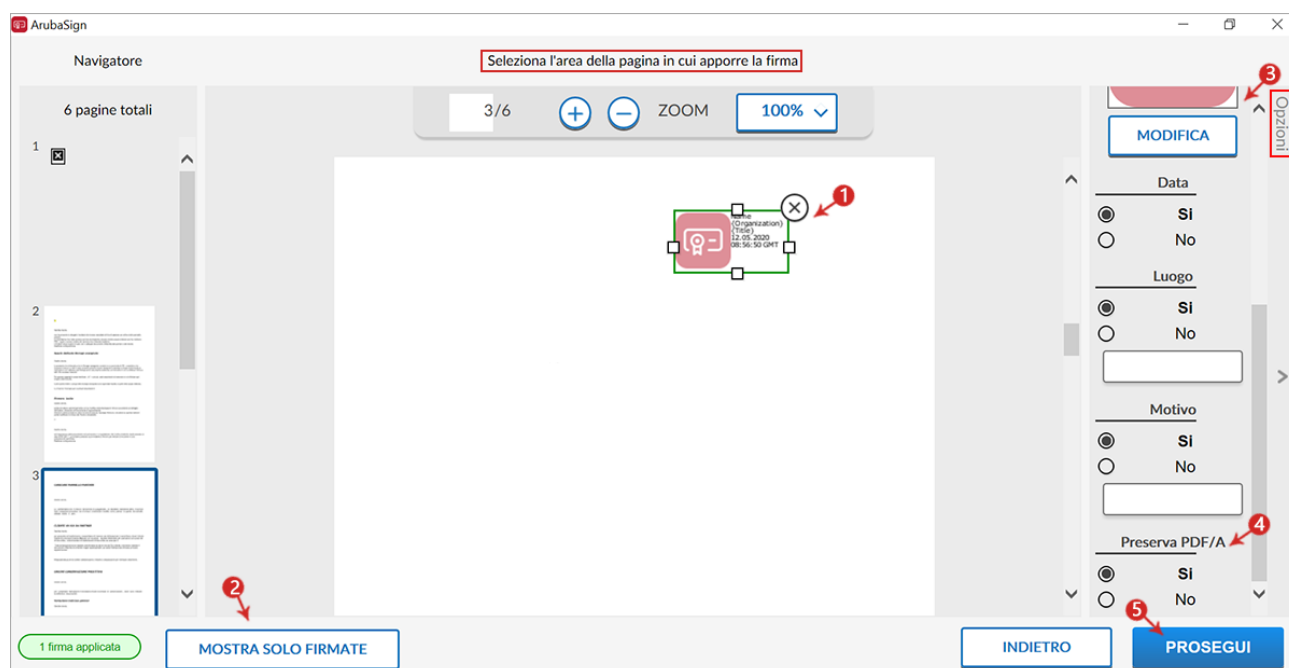
- 1) trascinare o selezionare uno o più documenti e/o una intera cartella;
- 2) il singolo/i documenti caricati/o sono visibili all'apposita schermata Documenti da firmare;
- 3) dal menu a tendina Seleziona il formato di firma selezionare come tipologia di Firma PAdES per firmare il file in formato .PDF e lasciare il Flag su Firma Grafica;
- 4) se in possesso di marche temporali, oltre alla firma, è possibile apporre al file una marcatura temporale;
- 5) dalla finestra Output rinominare, se desiderato, eventuali file prima di apporre la firma;
- 6) da CAMBIA CARTELLA verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
- 7) cliccare su PROSEGUI E FIRMA per continuare. Sono firmati tutti i documenti presenti alla finestra Documenti da firmare:



Alla schermata successiva:

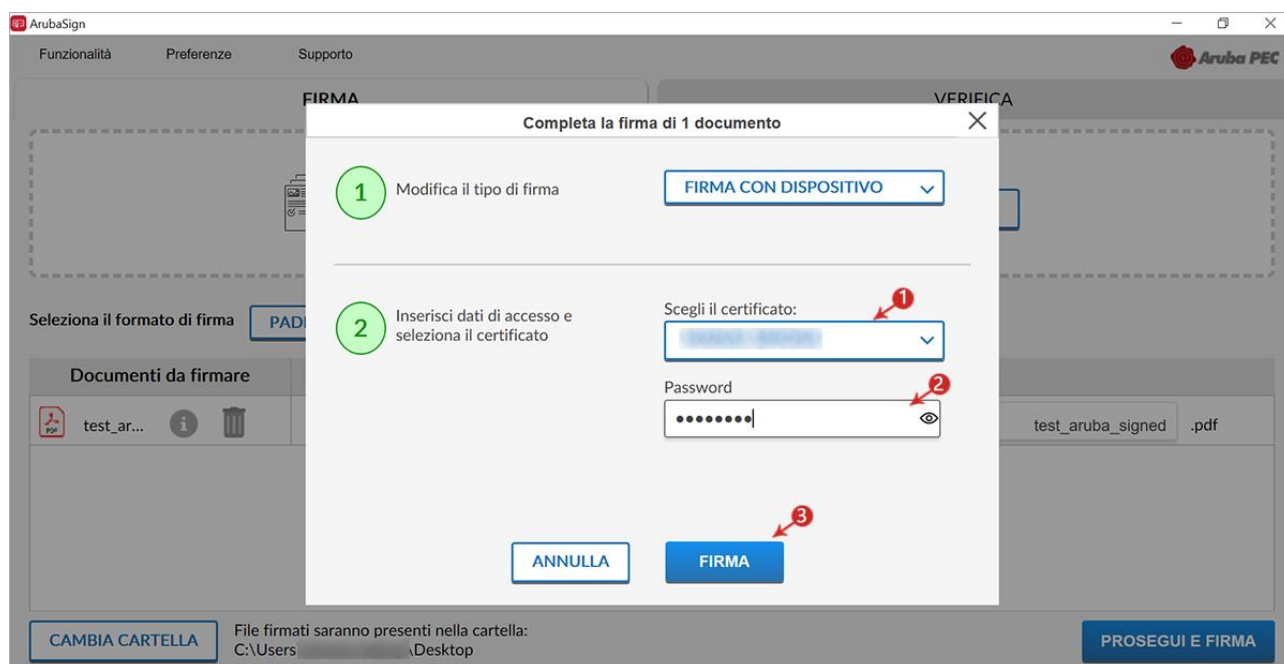
- 1) definire la posizione e la dimensione del campo che ospiterà la Firma Digitale;
- 2) è possibile visualizzare tutti i documenti o solo quelli firmati;
- 3) attraverso la finestra Opzioni sulla destra, è possibile caricare da locale, attraverso il tasto **MODIFICA**, una img in formato .gif/.jpg/.png da sostituire a quella presente di default per il timbro. L'immagine caricata è ridimensionata in scala rispetto alle dimensioni dell'area selezionata;
- 4) abilitando la funzione **Preserva PDF/A** la firma grafica è apposta preservando il formato stesso;
- 5) cliccare su **PROSEGUI** per procedere:

58



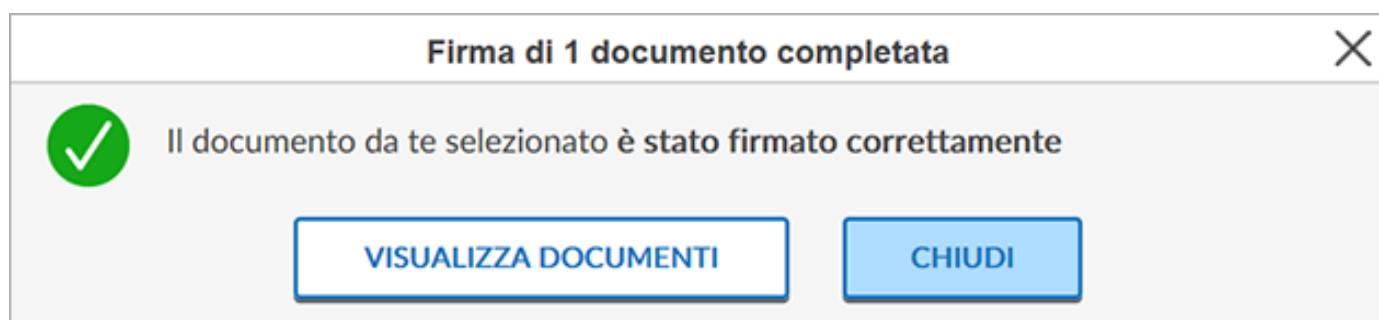
Alla schermata **Completa la firma di 1 documenti**:

- 1) assicurarsi che sia selezionato il Certificato per la firma digitale (in formato Cognome - Nome);
- 2) inserire il **PIN** di protezione della Smart Card;
- 3) cliccare su **FIRMA** per concludere il processo:



Al termine dell'operazione si visualizza la corretta firma del file.

Su **VISUALIZZA DOCUMENTI** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **CHIUDI** per terminare l'operazione:



Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al nome originale l'estensione **signed.pdf**.

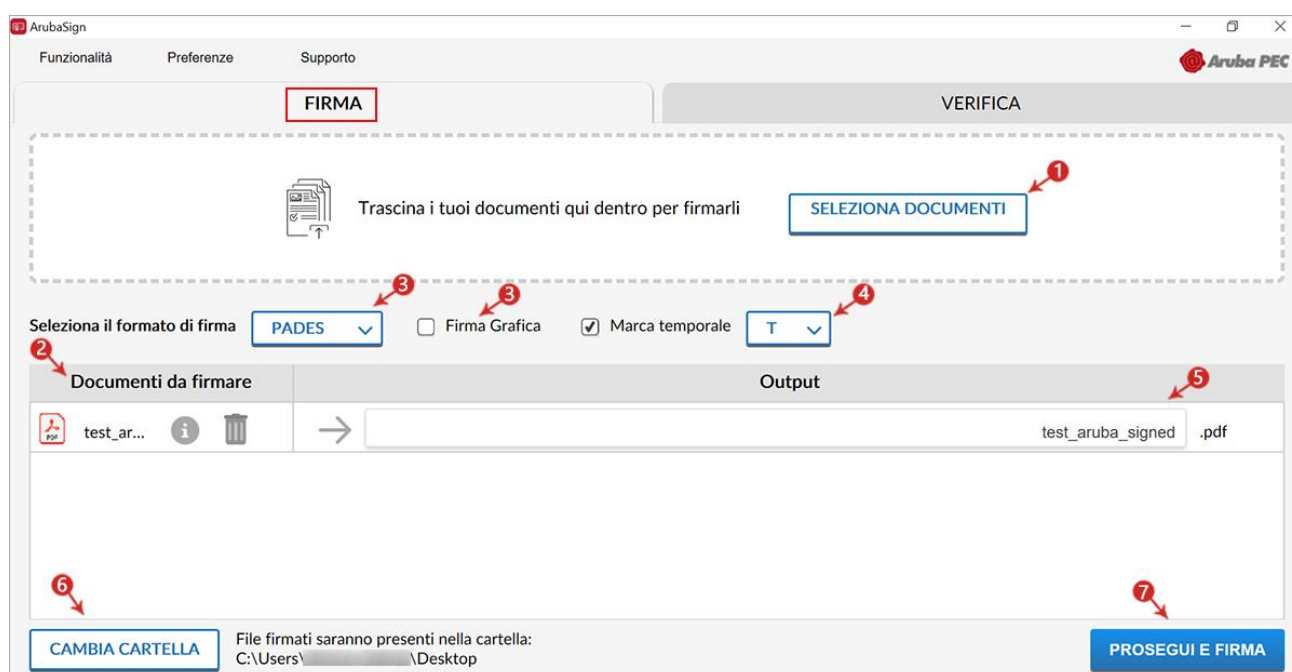
7.8 Apposizione Firma PDF – Invisibile - Firma Digitale

Il Formato di Firma **PAdES** è applicabile ai soli file **.PDF**, **.doc**, **.docx**, **.xls**, **.xlsx** (supporto a MS Word w MS Excel versione 2007 o superiore).

La Firma **PAdES - Firma Invisibile** consente di evitare l'inserimento dell'**appearance** (campo firma visibile) all'interno delle pagine del documento firmato.

Per **firmare digitalmente uno o più file in formato .PDF in formato PAdES - Firma Grafica** e/o una intera cartella **con Aruba Sign**:

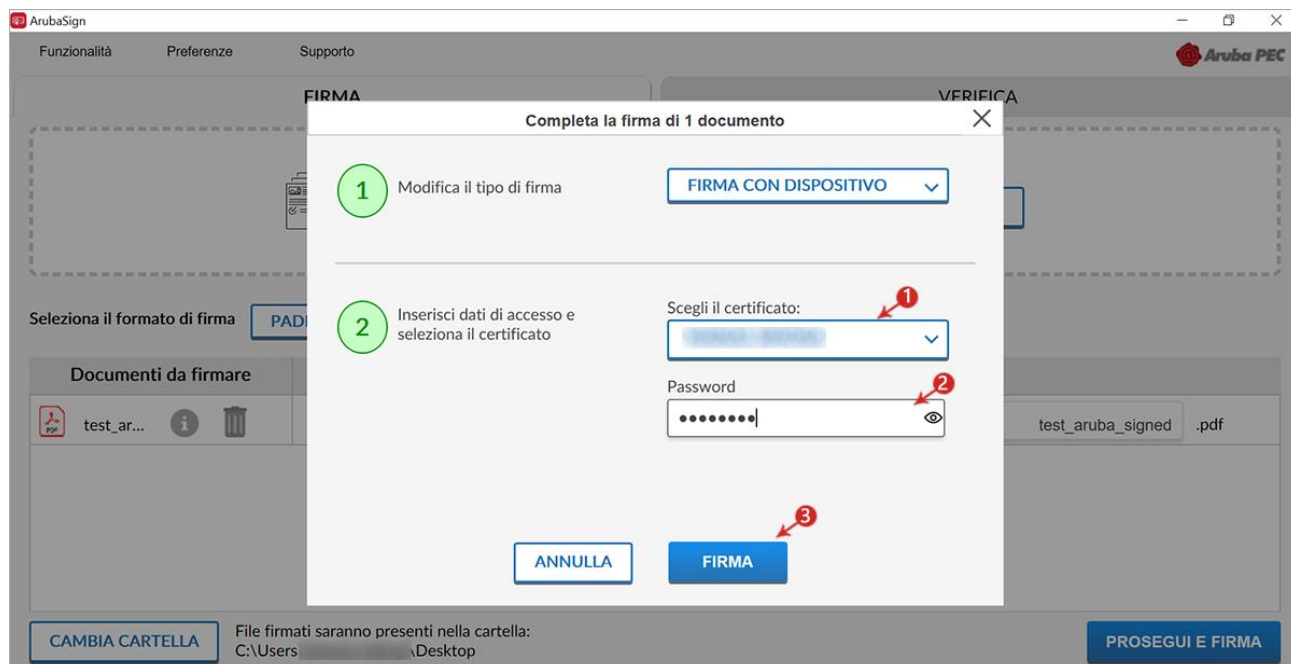
- 1) trascinare o selezionare uno o più documenti e/o una intera cartella;
- 2) il singolo/i documenti caricati/o sono visibili all'apposita schermata Documenti da firmare;
- 3) dal menu a tendina Seleziona il formato di firma selezionare come tipologia di Firma PAdES per firmare il file in formato .PDF e rimuovere il Flag su Firma Grafica;
- 4) se in possesso di Marche Temporal, oltre alla firma, è possibile apporre al file una marcatura temporale;
- 5) dalla finestra Output rinominare, se desiderato, eventuali file prima di apporre la firma;
- 6) da CAMBIA CARTELLA verificare che il percorso utilizzato per salvare il/i file firmato/i sia quello desiderato, o selezionarne uno nuovo utilizzando il pulsante indicato;
- 7) cliccare su PROSEGUI E FIRMA per continuare. Sono firmati tutti i documenti presenti alla finestra Documenti da firmare:



Alla schermata **Completa la firma di documenti:**

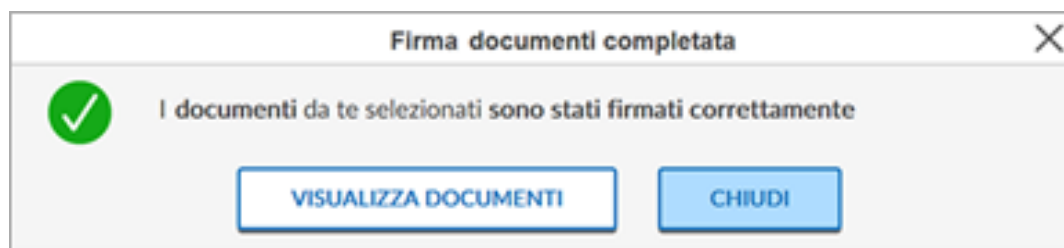
- 1) assicurarsi che sia selezionato il Certificato per la firma digitale (in formato Cognome - Nome);
- 2) inserire il PIN di protezione della Smart Card;

3) cliccare su **FIRMA** per concludere il processo:



Al termine dell'operazione si visualizza la corretta firma del file.

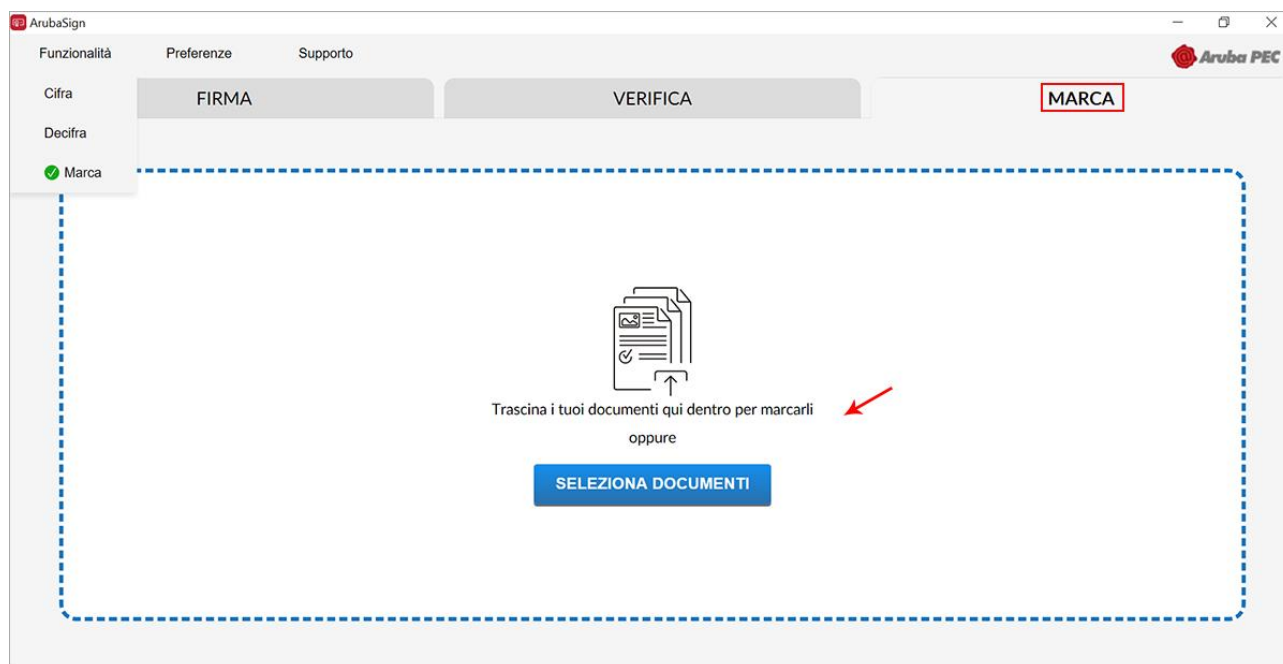
Su **VISUALIZZA DOCUMENTI** sono visibili i documenti firmati e salvati in formato .p7m, cliccare su **CHIUDI** per terminare l'operazione:



Il documento firmato viene salvato nella cartella indicata durante il processo, aggiungendo al nome originale l'estensione **signed.pdf**.

7.9 Apposizione di Marche Temporalì - Firma Digitale

Per apporre una Marca Temporale accedere su **Funzionalità** e poi su **Marca**, se non precedentemente configurato verrà popolato sulla destra la scheda, quindi trascinare o selezionare il file che si desidera cifrare:



Alla pagina visualizzata:

4) selezionare il formato di salvataggio della marca temporale. È possibile scegliere tra:

- **TSR:** Il File creato contiene solo l'impronta del file, non tutto il file, e **la marca temporale in formato TSR è separata dal documento**. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso. Se si appone una marca temporale in formato TSR e si desidera inviarla a un destinatario, è necessario inviare anche il documento di origine.
- **TSD:** Il File creato comprende sia **il file sottoposto a marcatura che la marcatura temporale stessa**. Se si appone una marca temporale in formato TSD e si desidera inviarla a un destinatario, non è necessario inviare anche il documento di origine.

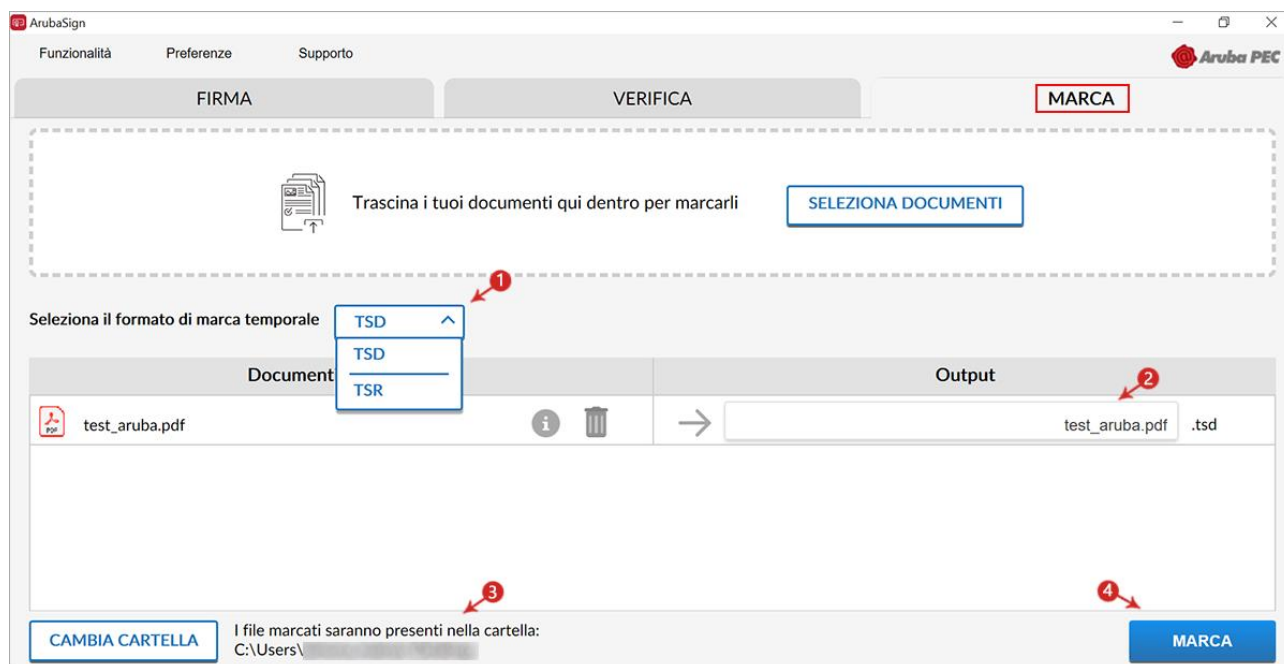
Gli altri dati (password e cartella di destinazione del file) sono indicati automaticamente del sistema:

- la **password** è preimpostata a seguito della configurazione dell'Account di marcatura Temporale;
- il **percorso di destinazione del File** inserito è la cartella su cui risiede il file originale.

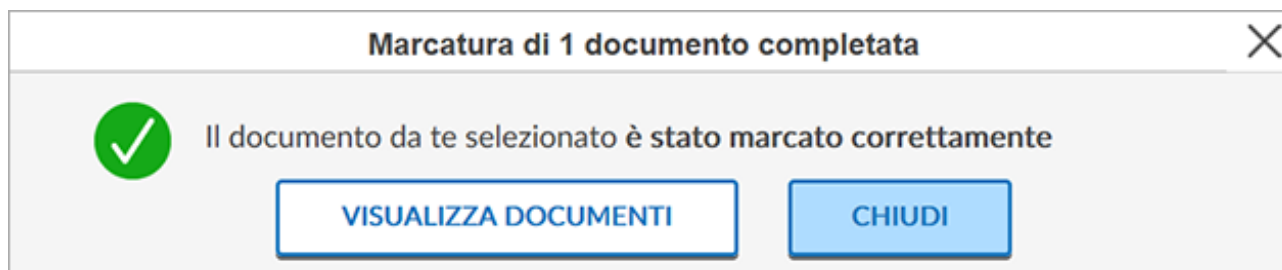
5) dalla finestra **Output** rinominare, se desiderato, eventuali file prima di apporre la firma;

6) il documento è disponibile nella cartella indicata in fase di apposizione della marcatura stessa;

7) cliccare **MARCA** al messaggio che notifica la corretta marcatura del file per completare l'operazione:

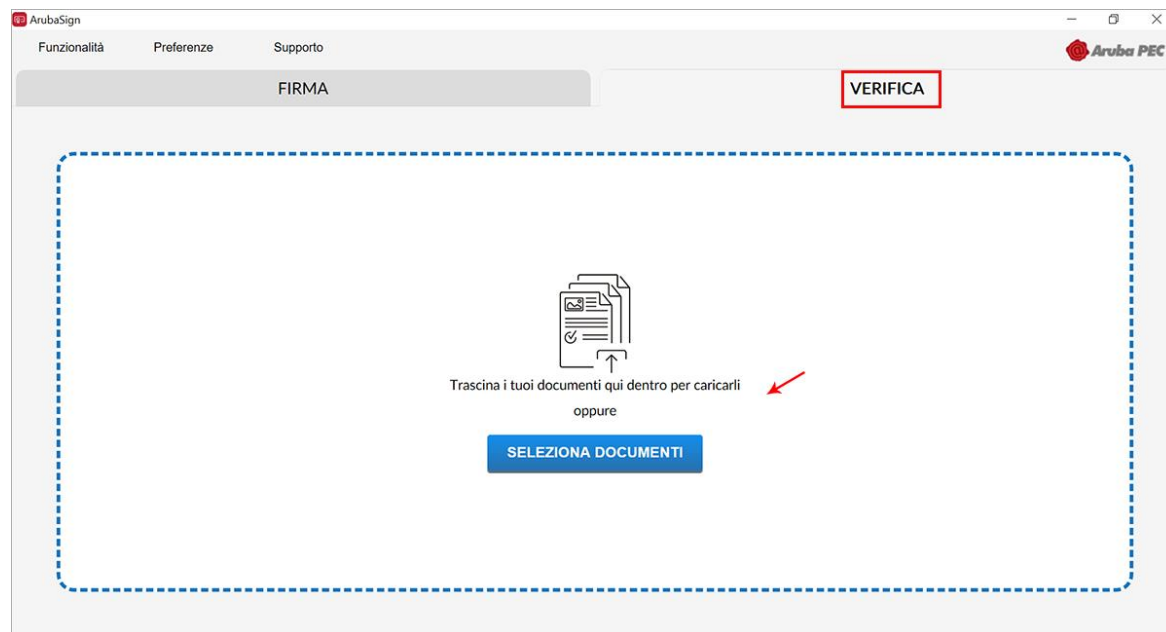


Il file è disponibile nella cartella indicata in fase di apposizione della marcatura stessa. Cliccare **CHIUDI** per completare l'operazione:



7.10 Verifica di file firmati - Firma Digitale

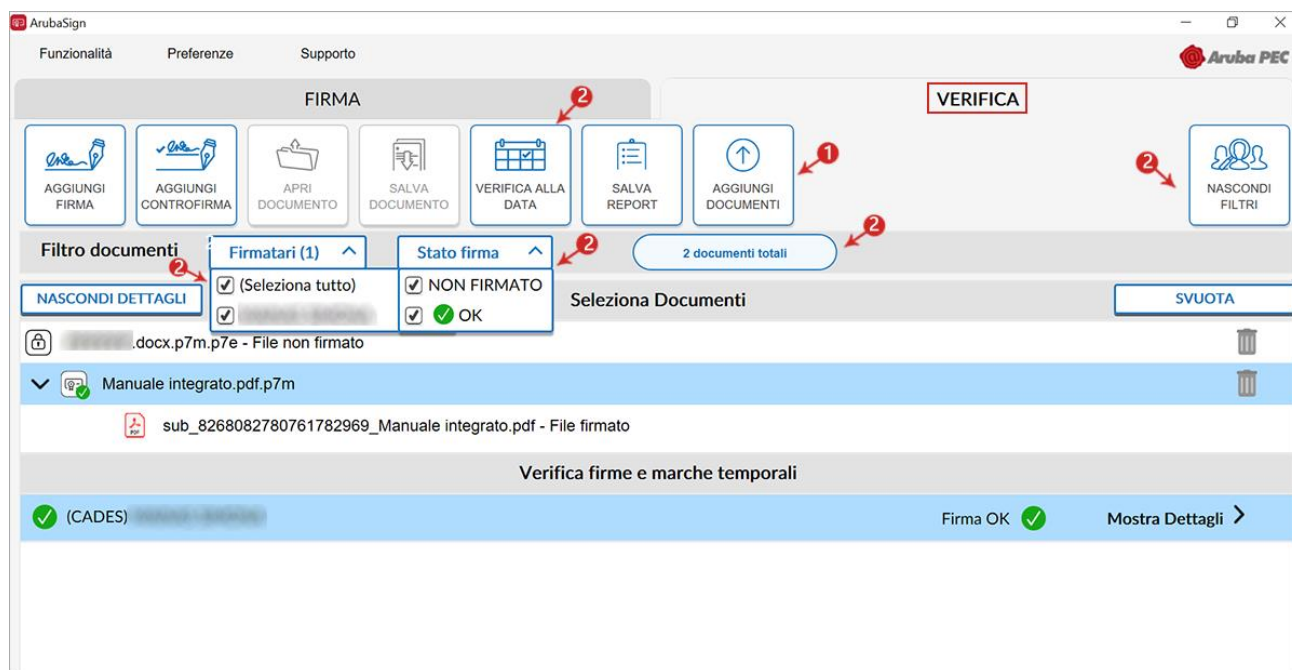
Per verificare uno o più file firmati con Aruba Sign, trascinare o selezionare il documento nella scheda **VERIFICA**:



Alla schermata visualizzata è possibile:

- 1) verificare ulteriori file firmati trascinandoli da locale o su **AGGIUNGI DOCUMENTO**;
- 2) da **Mostra/Nascondi Filtri** sono riportati il nome e cognome del/i firmatario/i, il numero di firme che ha apposto, la data dell'ultima apposizione e lo **Stato** (esito) della verifica. Per visionare quali sono i documenti firmati da uno specifico firmatario, inserire il flag in corrispondenza del soggetto interessato, il nome appare a fianco dei singoli file che ha firmato presenti nell'area **Seleziona documenti**:

64



3) **verifica firme e Marche Temporal** sono visibili le firme presenti all'interno del file;

- **Firma valida**

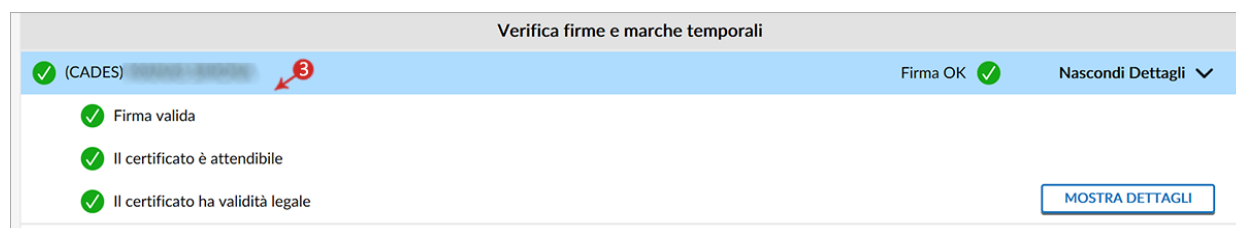
Attesta il formato della firma e che il documento non è stato alterato dopo la firma;

- **Il certificato è attendibile**

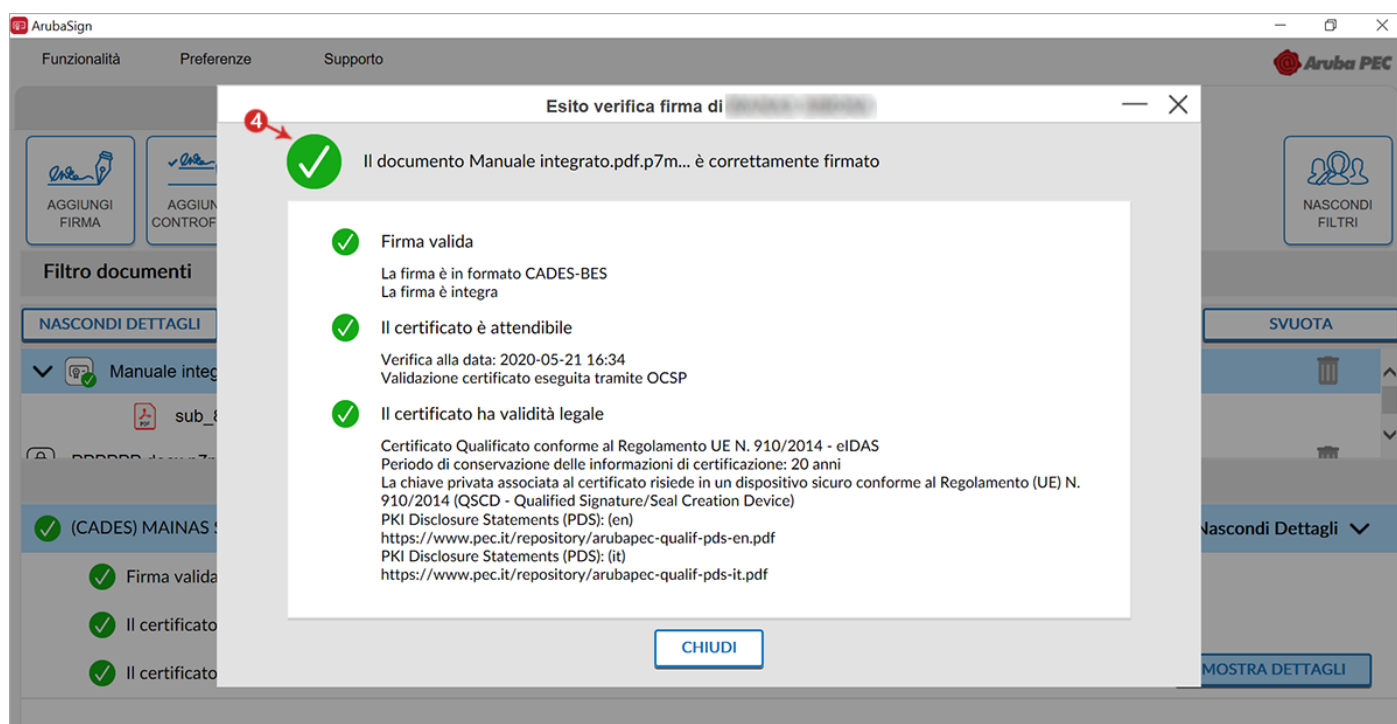
Il messaggio indica che il certificato del sottoscrittore è garantito da una Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori e che non risulta scaduto alla data della Verifica;

- **Il certificato ha validità legale**

Attesta che il certificato del sottoscrittore è un certificato di Firma Digitale qualificato:



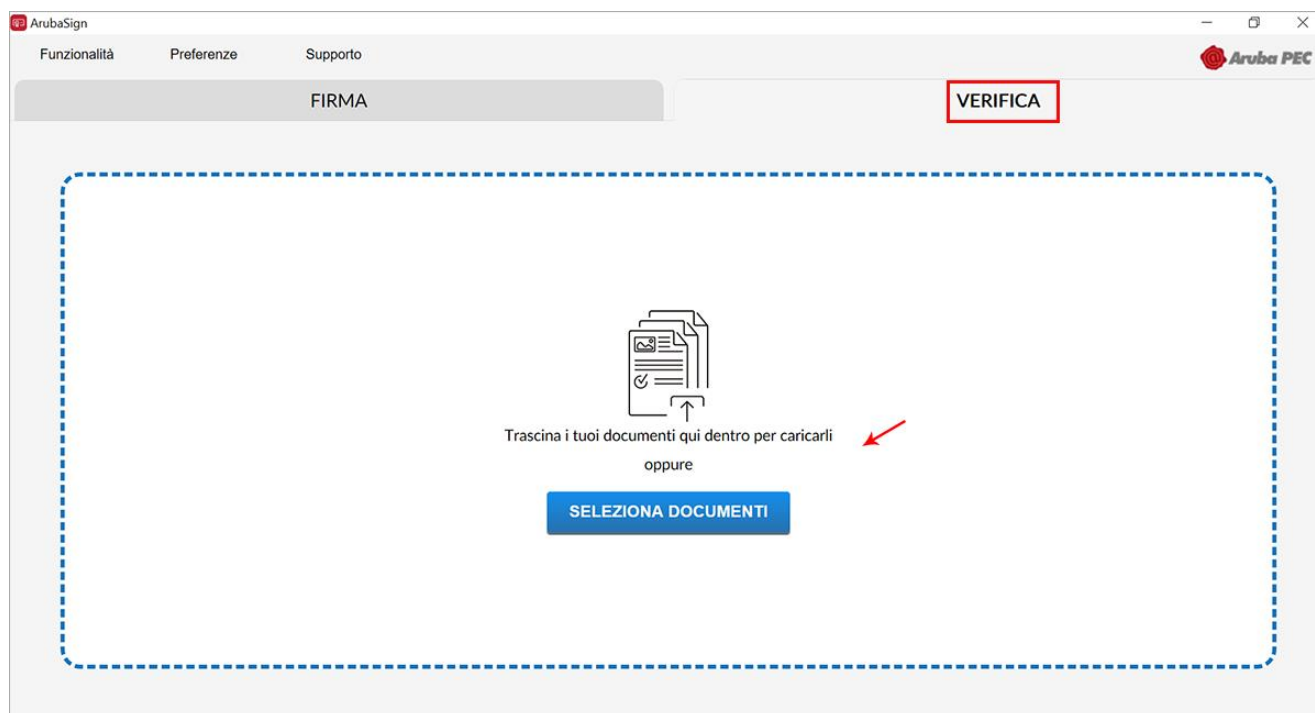
Da **Dettagli firma/marca** è possibile verificare la validità della firma apposta, in particolare:



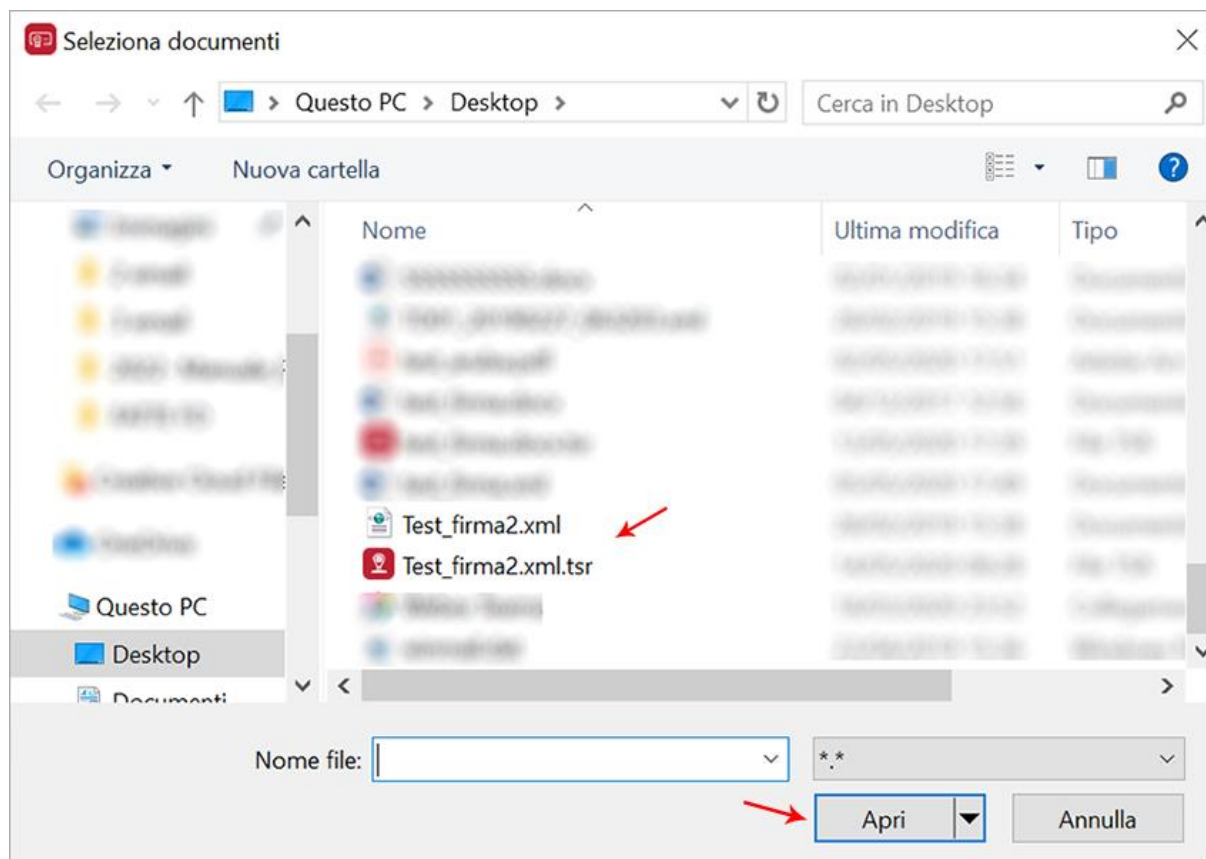
7.11 Verifica di Marca Temporale in formato TSR - Firma Digitale

Una Marca Temporale in formato **TSR** è **separata dal documento** su cui è apposta. Pertanto, per verifica il file TSR, è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSR stesso.

Per verificare uno o più File marcati in formato TSR con Aruba Sign, trascinare o selezionare il documento all'interno della scheda **VERIFICA**:

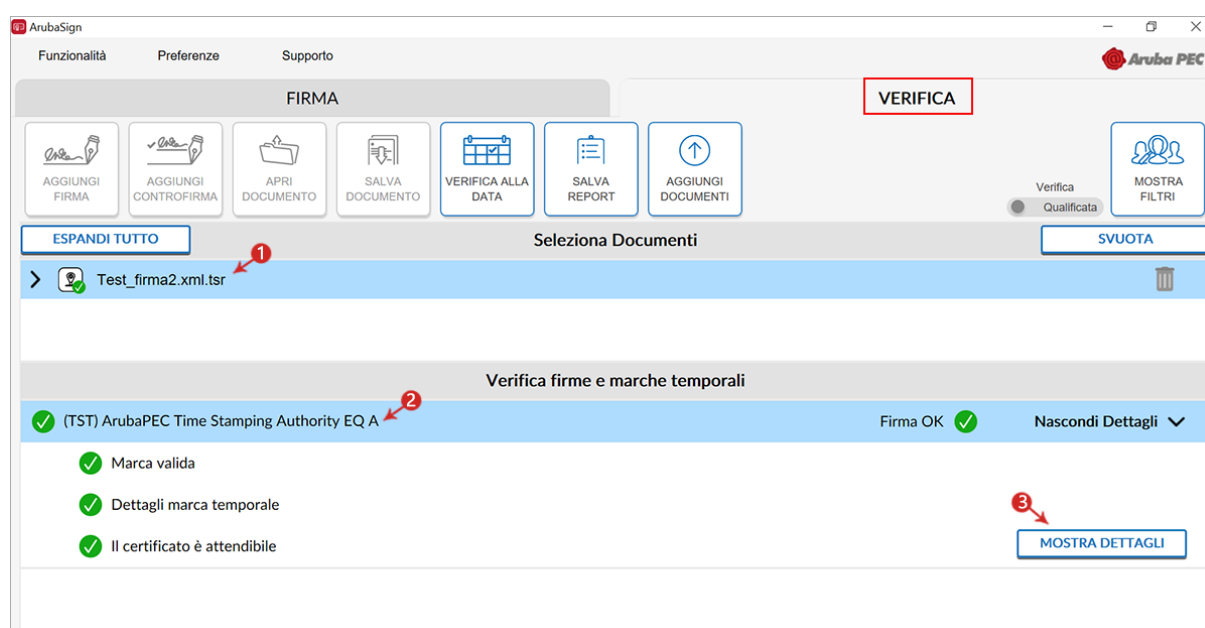


Selezionare da locale il file originario e il file associato alla marca stessa, quindi cliccare su **Apri**:



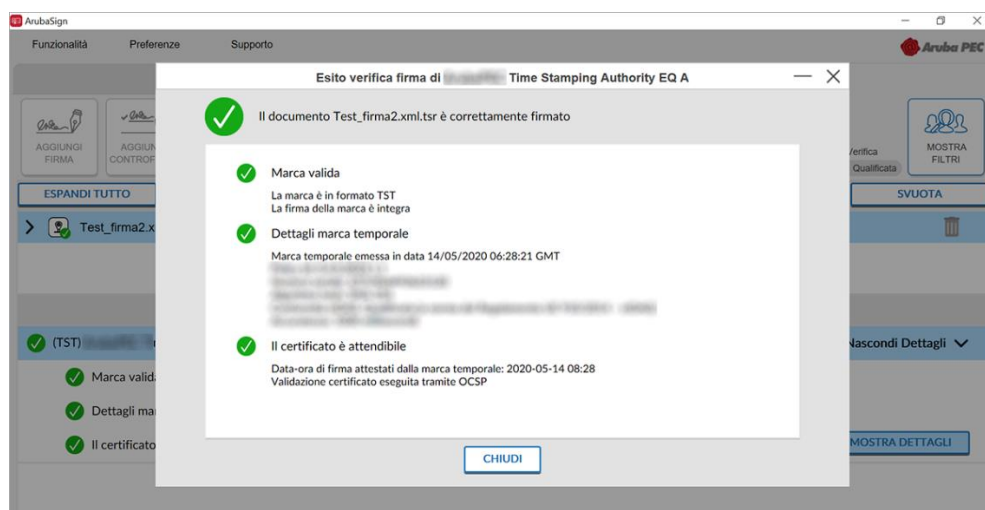
Alla schermata visualizzata è possibile:

- 1) visualizzare il file marcato;
- 2) su **Verifica firme e marche temporali** sono visibili le marche presenti all'interno del file;
 - **Marca valida**
Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;
 - **Dettagli marca temporale**
Sono riportate le specifiche della marca stessa;
 - **Il certificato è attendibile**
Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori;



67

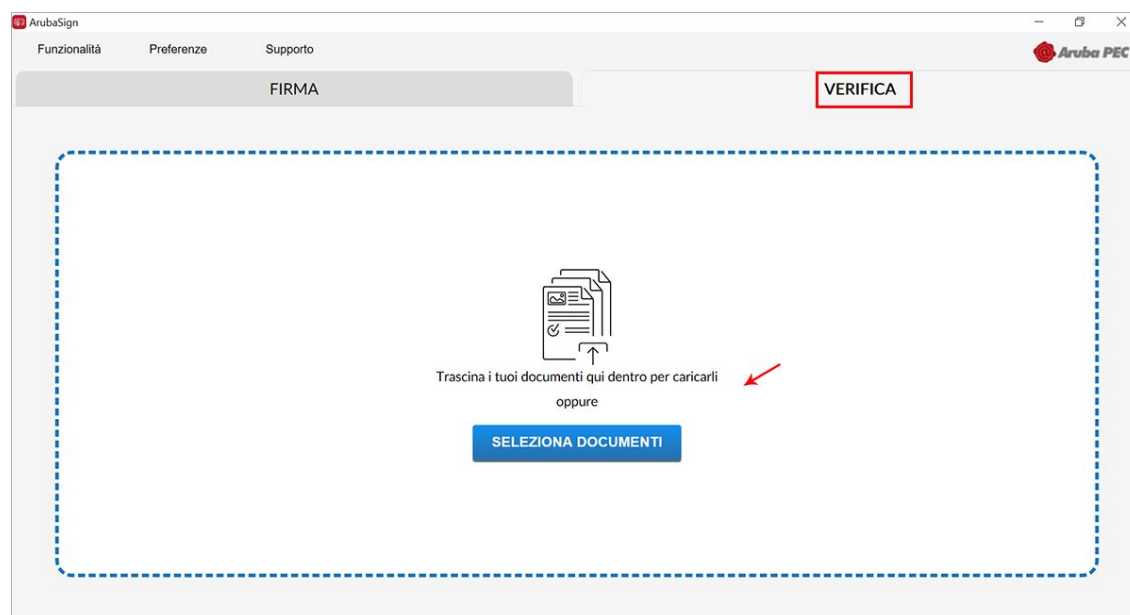
- 3) Da **MOSTRA DETTAGLI** è possibile verificare la validità della firma apposta:



7.12 Verifica di Marca Temporale in formato TSD - Firma Digitale

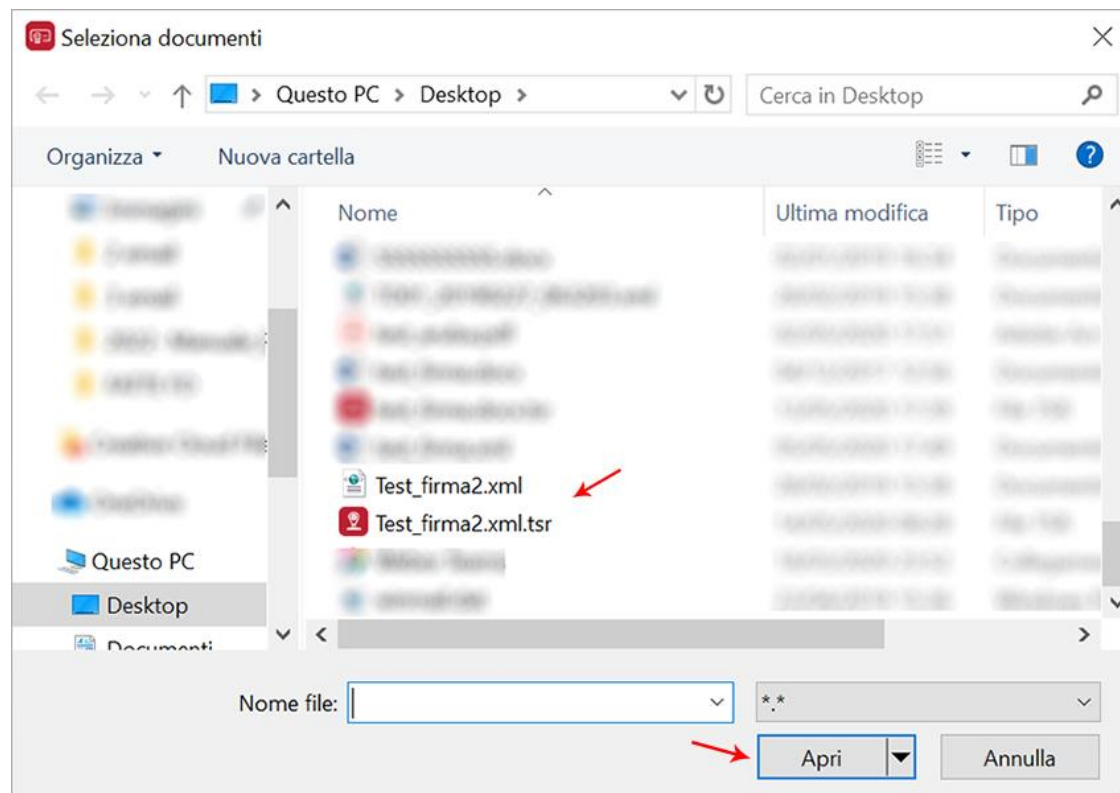
Una Marca Temporale in **formato TSD comprende** sia il file sottoposto a marcatura che la marcatura temporale stessa. Pertanto, per verificare il file TSD, non è indispensabile possedere anche il documento sottoposto a marca temporale, e che ha generato il TSD stesso.

Per verificare uno o più File marcati in formato TSD con Aruba Sign, trascinare o selezionare il documento all'interno della scheda **VERIFICA**:



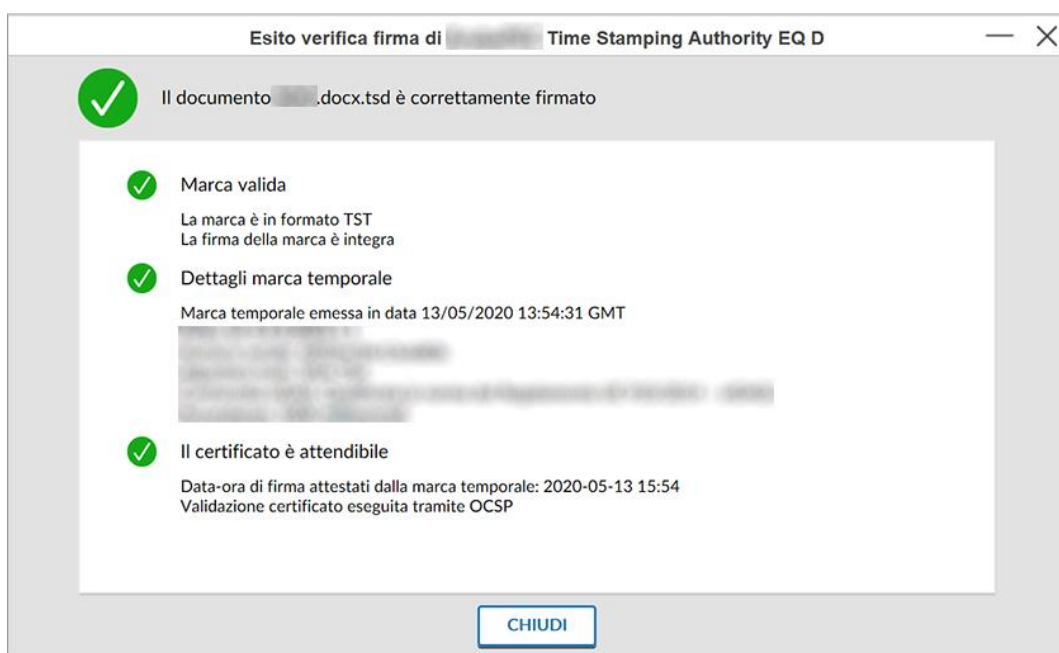
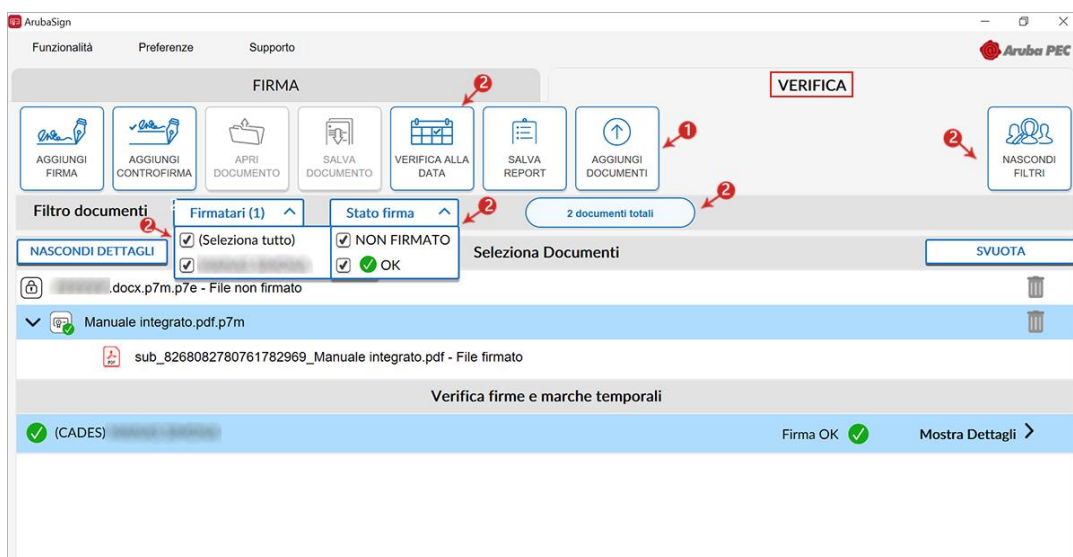
68

Selezionare da locale il file associato alla marca stessa, quindi cliccare su **Apri**:



Alla schermata visualizzata è possibile:

- 1) visualizzare il file marcato;
- 2) su **Verifica firme e marche temporali** sono visibili le marche presenti all'interno del file;
 - Marca valida
Indica che la marca temporale è integra ed è correttamente associata al documento selezionato;
 - Dettagli marca temporale
Sono riportate le specifiche della marca stessa;
 - Il certificato è attendibile
Attesta che la Marca Temporale è rilasciata da un'Autorità di Certificazione inclusa nell'Elenco Pubblico dei Certificatori;
- 3) Da **MOSTRA DETTAGLI** è possibile verificare la validità della firma apposta:



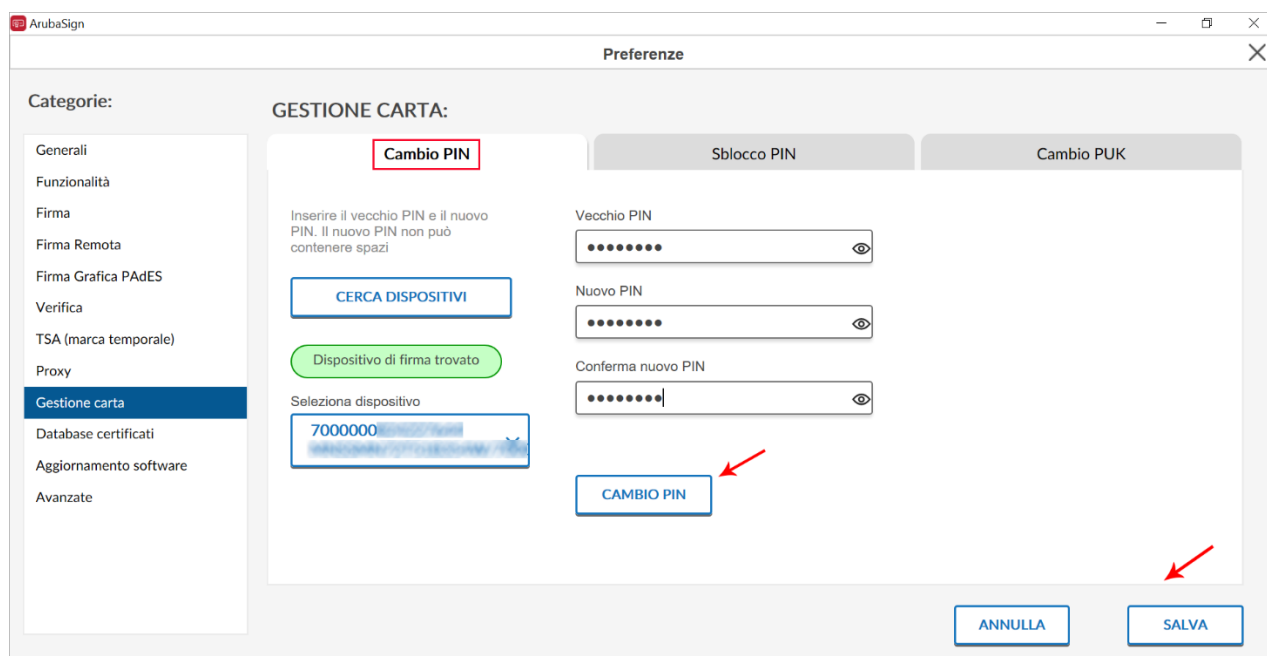
8 Funzioni disponibili Home Page Aruba Sign

8.1 Gestione Carta Aruba Sign (PC) - modifica PIN e PUK

Per cambiare il **codice PIN** della Smart Card, tramite l'utilizzo di un Kit di Firma Digitale, accedere su **Gestione Carta** del Software Aruba Sign.

Al Tab **Cambio PIN** inserire:

- PIN precedente;
- impostare e confermare un **nuovo codice PIN**;
- cliccare su **Cambio PIN** e poi su **SALVA**:

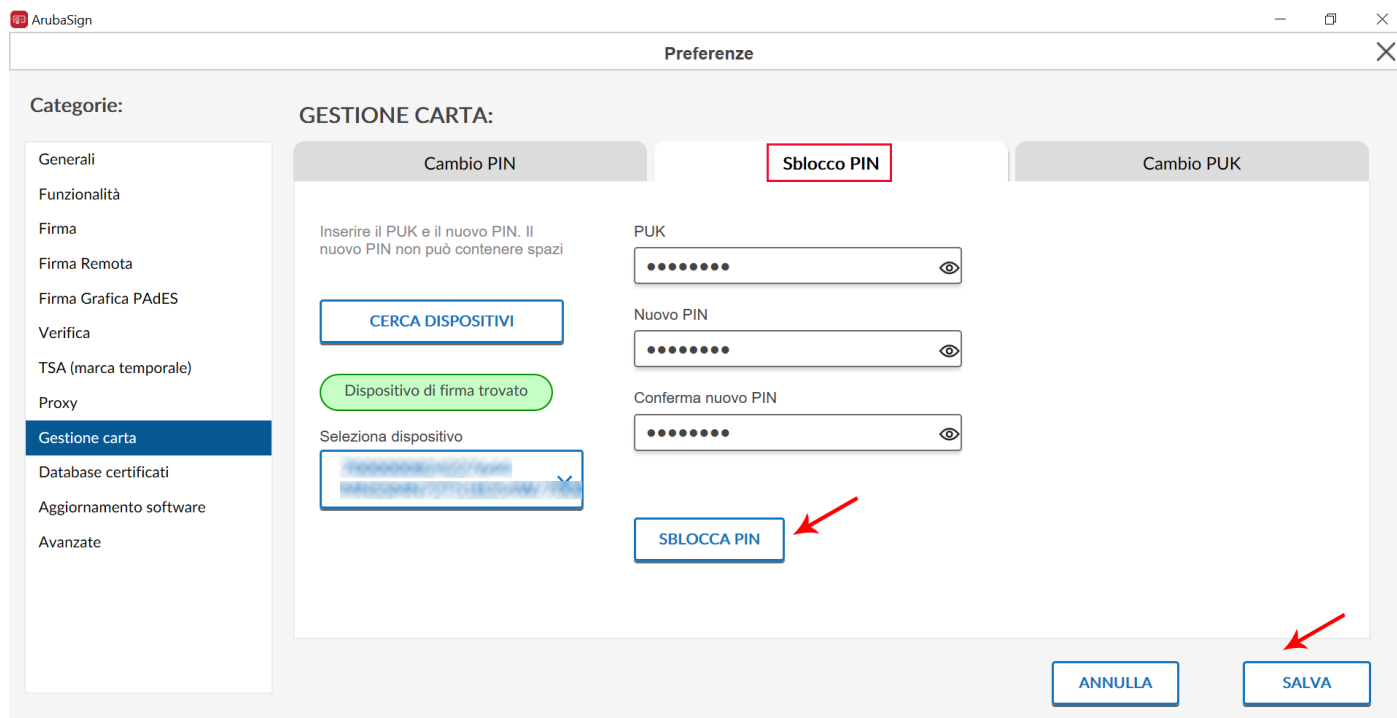


70

Per sbloccare il **codice PIN** della Smart Card, tramite l'utilizzo di un Kit di Firma Digitale, accedere su **Gestione Carta** del Software Aruba Sign.

Al Tab **Sblocco PIN** inserire:

- codice PUK della Smart Card;
- impostare e confermare un nuovo **codice PIN**;
- cliccare su **Sblocca PIN** e poi su **SALVA**:



ArubaSign

Preferenze

Categorie:

- Generali
- Funzionalità
- Firma
- Firma Remota
- Firma Grafica PAdES
- Verifica
- TSA (marca temporale)
- Proxy
- Gestione carta**
- Database certificati
- Aggiornamento software
- Avanzate

GESTIONE CARTA:

Cambio PIN

Sblocco PIN

Cambio PUK

Inserire il PUK e il nuovo PIN. Il nuovo PIN non può contenere spazi

CERCA DISPOSITIVI

Dispositivo di firma trovato

Seleziona dispositivo

PUK

NUOVO PIN

Conferma nuovo PIN

SBLOCCA PIN

ANNULLA

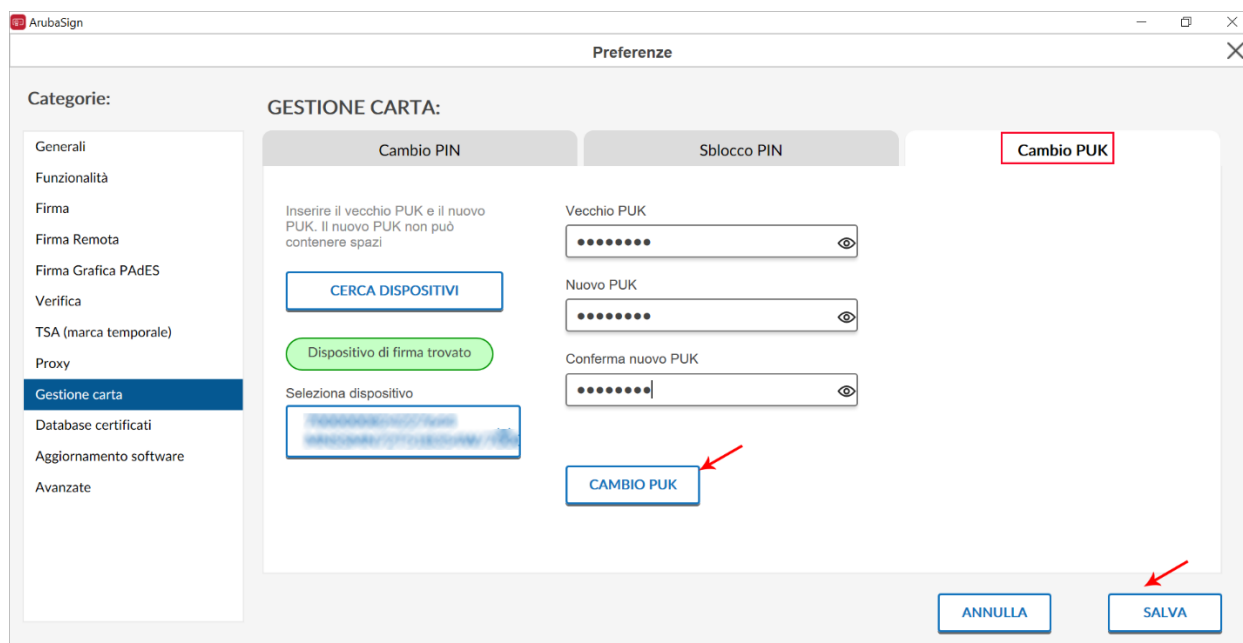
SALVA

Per cambiare il **codice PUK** della Smart Card, tramite l'utilizzo di un Kit di Firma Digitale, accedere su "Gestione Carta" del Software Aruba Sign:

Al Tab **Cambio PUK** inserire:

- vecchio Codice PUK della Smart Card;
- impostare e confermare un nuovo **codice PUK**;
- cliccare su **Cambio PUK** e poi su **SALVA**:

71



ArubaSign

Preferenze

Categorie:

- Generali
- Funzionalità
- Firma
- Firma Remota
- Firma Grafica PAdES
- Verifica
- TSA (marca temporale)
- Proxy
- Gestione carta**
- Database certificati
- Aggiornamento software
- Avanzate

GESTIONE CARTA:

Cambio PIN

Sblocco PIN

Cambio PUK

Inserire il vecchio PUK e il nuovo PUK. Il nuovo PUK non può contenere spazi

CERCA DISPOSITIVI

Dispositivo di firma trovato

Seleziona dispositivo

Vecchio PUK

NUOVO PUK

Conferma nuovo PUK

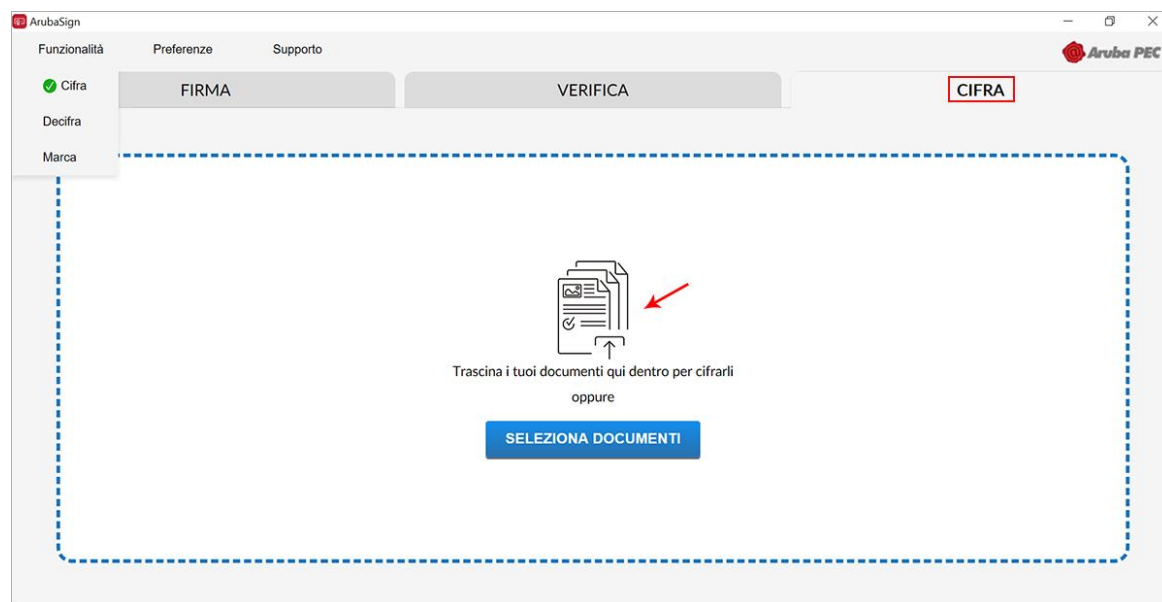
CAMBIO PUK

ANNULLA

SALVA

8.2 Cifra e Decifra un file Aruba Sign (PC)

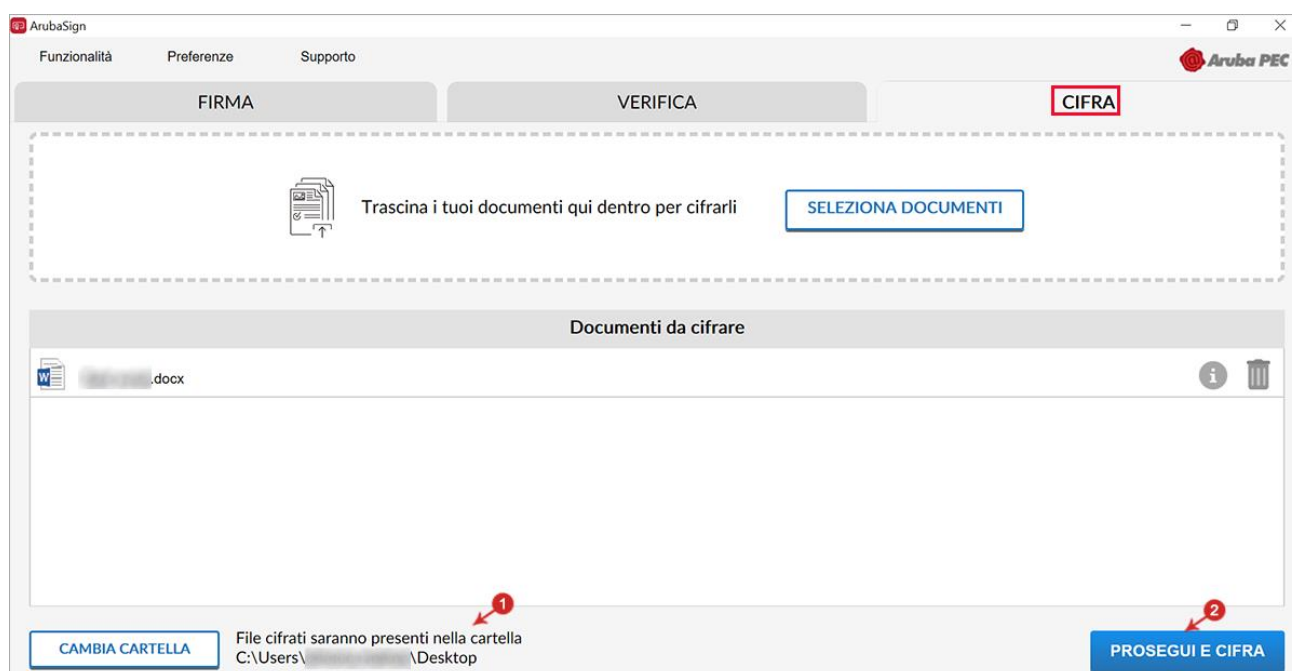
Per cifrare un File con Software di Firma Aruba Sign, esportare il Certificato di Autenticazione CNS in formato .cer, accedere su **Funzionalità** e poi su **Cifra**, se non precedentemente configurato verrà popolato sulla destra la scheda, quindi trascinare o selezionare il file che si desidera cifrare:



Una volta caricato il file, lo stesso è visibile nella finestra **Documenti da cifrare**. Per procedere:

- 1) Verificare la correttezza del percorso su cui salvare il file cifrato, o selezionare una nuova cartella utilizzando il pulsante indicato in figura;
- 2) Spuntare su PROSEGUI E CIFRA:

72

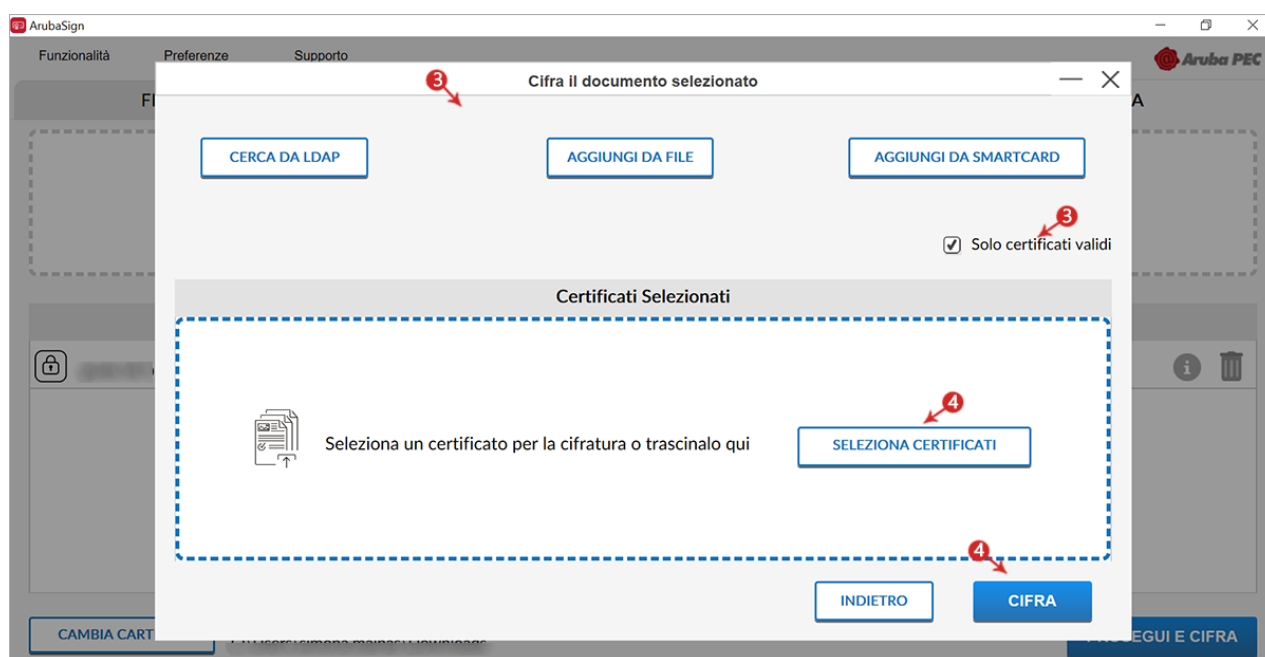


3) Nella schermata successiva è possibile scegliere 3 diverse modalità per cercare un certificato:

- CERCA DA LDAP
- AGGIUNGI DA FILE
- AGGIUNGI DA SMARTCARD

In alternativa selezionare attraverso la spunta solo i certificati validi.

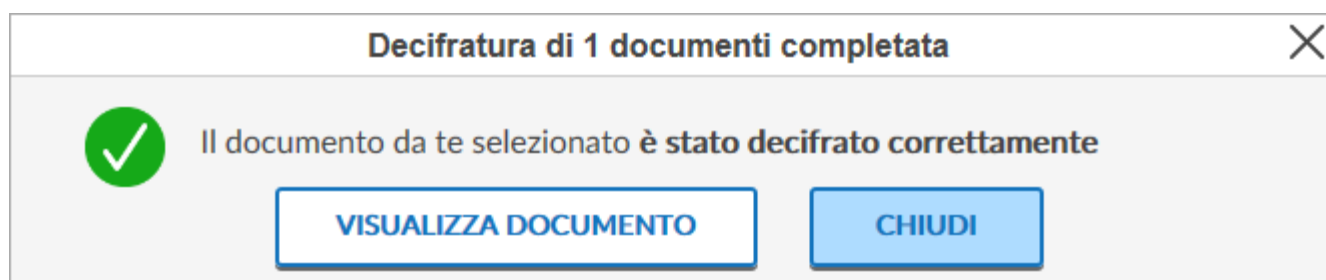
4) È possibile inoltre su **SELEZIONA CERTIFICATO** ricercare all'interno delle cartelle presenti nel PC dei certificati e infine cliccare su **CIFRA**:



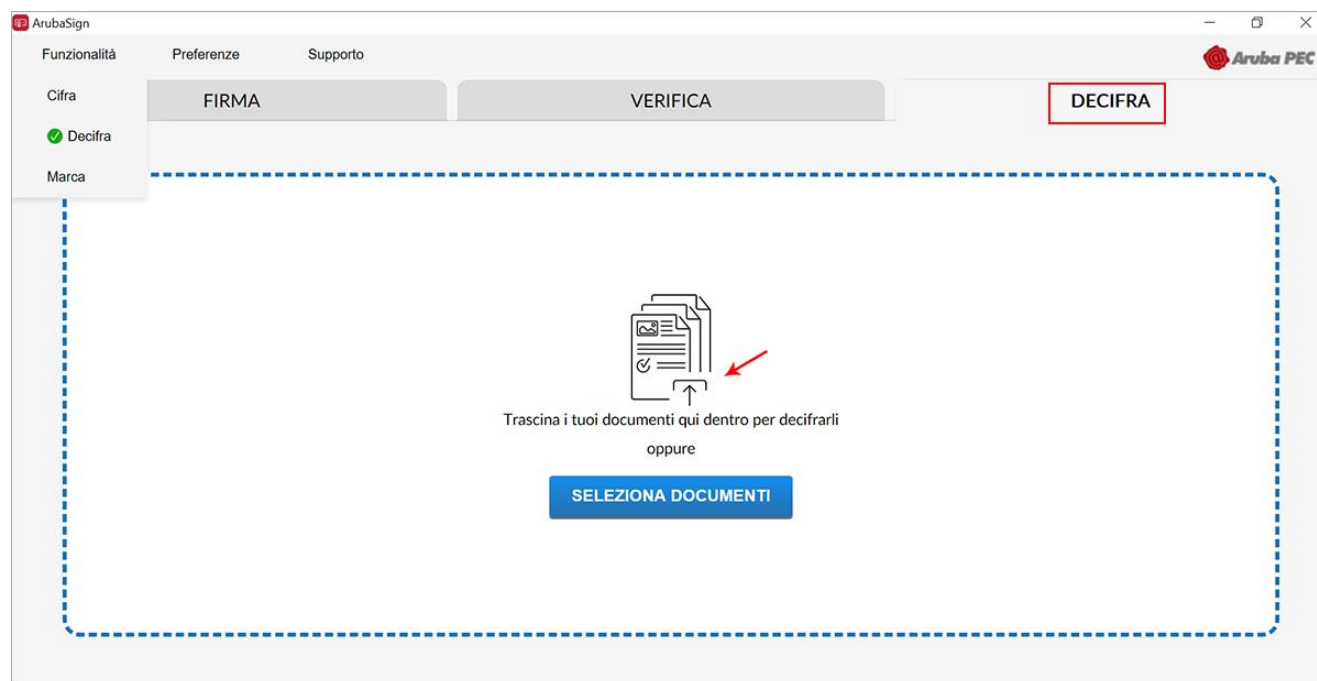
73

Il programma di cifratura crea un file con estensione .p7e che include il file originale. Il documento è visibile nella cartella di destinazione indicata in fase di creazione.

Se l'operazione è stata eseguita correttamente si visualizza la seguente schermata di conferma. Cliccare su **CHIUDI**:



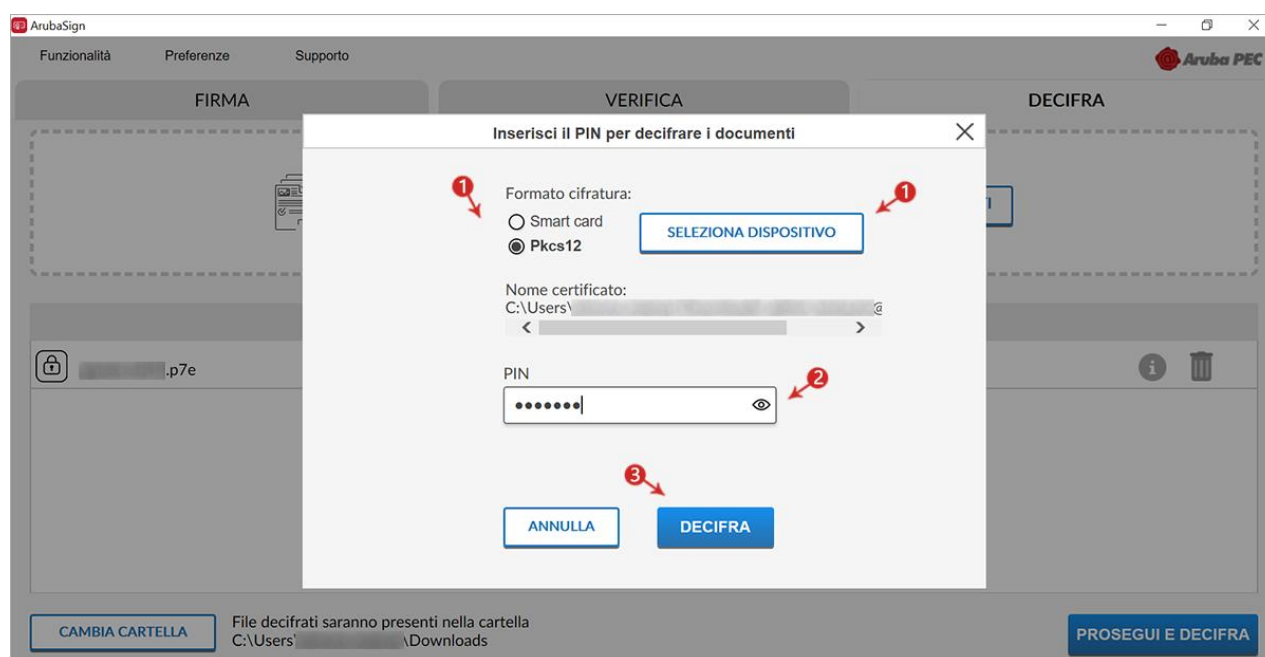
Per decifrare un File con Software di Firma Digitale Aruba Sign, trascinare o selezionare il file cifrato (formato .p7e) nella sezione **Decifra**:



Aruba sign verifica che nella Smart Card sia presente almeno uno dei certificati indicati nella fase di cifratura. Alla schermata visualizzata:

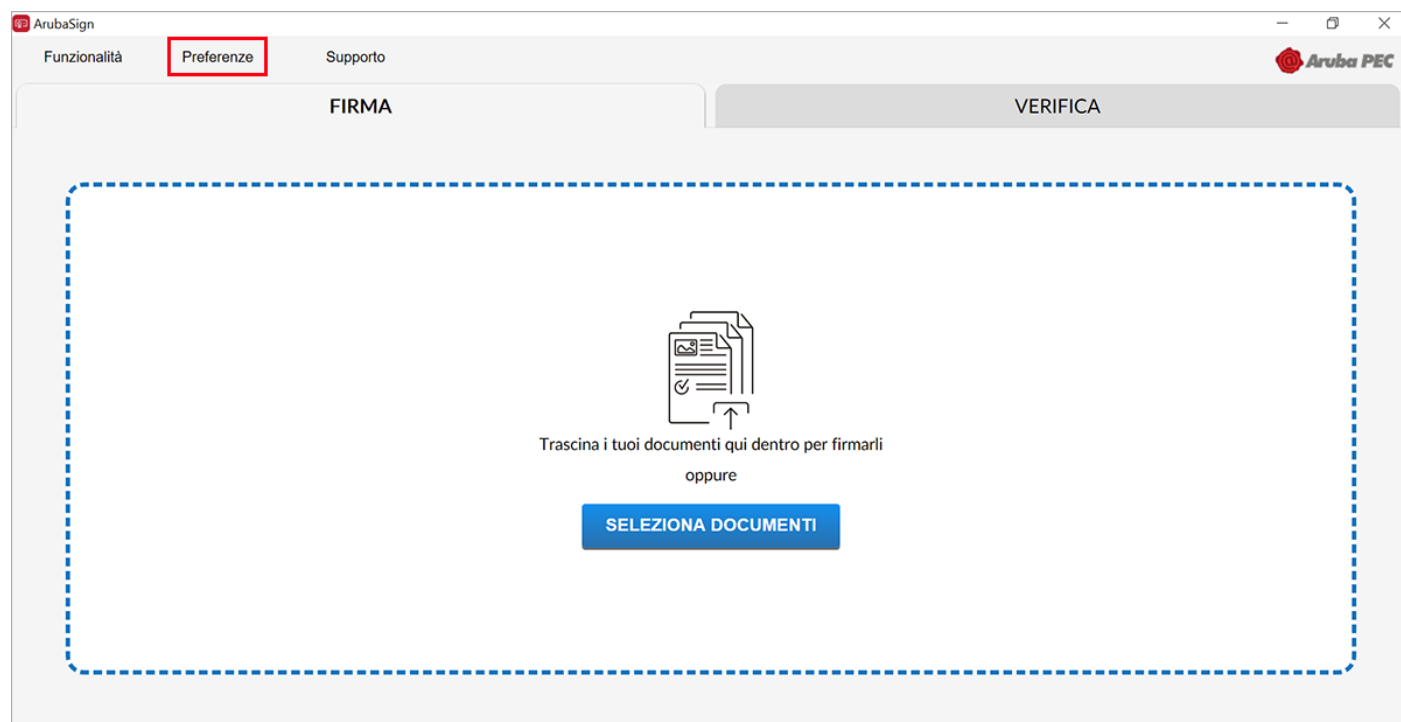
- 1) È possibile scegliere l'opzione **Smart card o Pkcs12** in questo caso selezionare il dispositivo;
- 2) Inserire il **PIN** della Smart Card stessa;
- 3) Cliccare su **DECIFRA** per proseguire:

74



8.3 Configurazione Proxy http Aruba Sign

La Configurazione dei Parametri **Proxy HTTP**, tramite l'utilizzo del Software Aruba Sign, permette di svolgere le operazioni di verifica di un file firmato, aggiornamento, controllo, stato di revoca e richiesta di Marche Temporalì qualora la postazione si trovi dietro Proxy HTTP. Per procedere, aprire il menu **Preferenze** di Aruba Sign:



75

Quindi allo specifico Tab **Proxy** è possibile scegliere:

- Nessun Proxy
- Configurazione Manuale
- Configurazione di sistema

Se si sceglie la Configurazione manuale impostare i relativi parametri e salvarli:

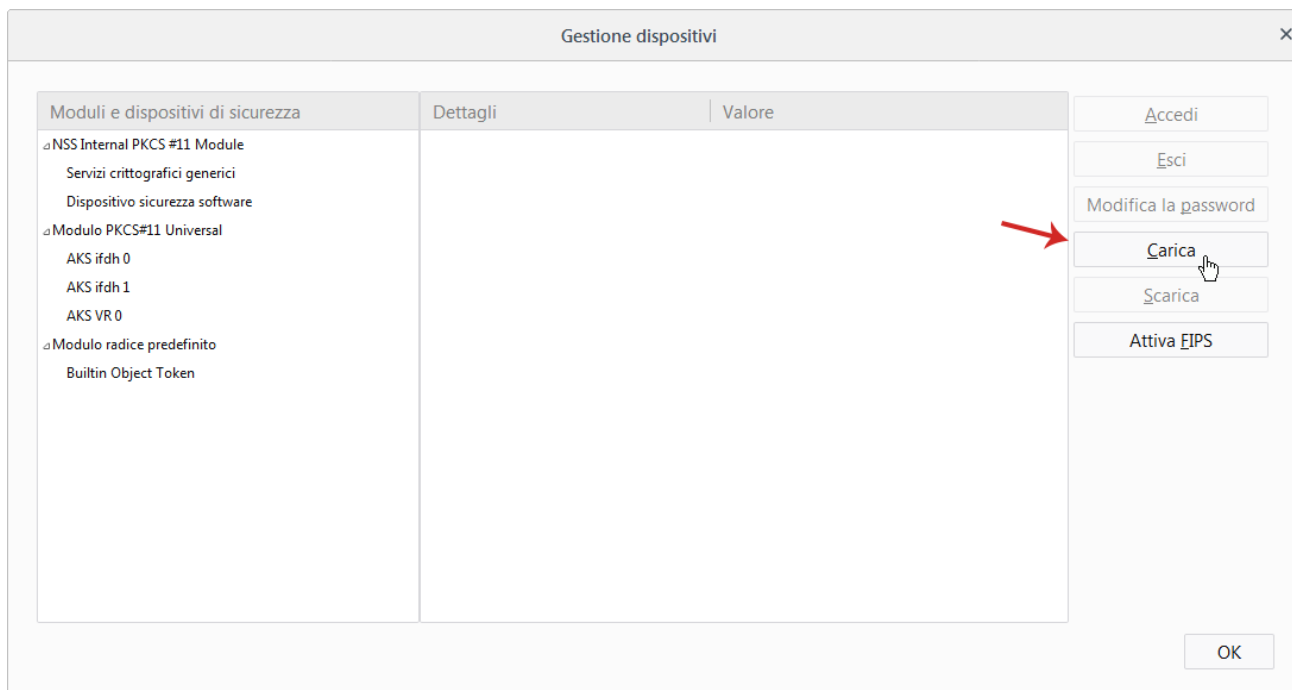
- **Proxy Url:** 192.168.1.1
- **Proxy Port:** 8080
- **Proxy User:** Nome utente
- **Proxy Password:** Password

9 Import Certificato su Mozilla Firefox Firma Digitale (PC)

La funzione **Import Certificato** per Aruba Sign è automatica su **Internet Explorer** e **Google Chrome**. Di seguito le modalità per **eseguire manualmente l'Import Certificato su Mozilla Firefox e abilitare l'utilizzo del Browser installato localmente su PC a cui è collegato il dispositivo**. Per procedere:

- 1) Avviare Mozilla Firefox;
- 2) Dall'icona Strumenti in alto a destra, scegliere Opzioni;

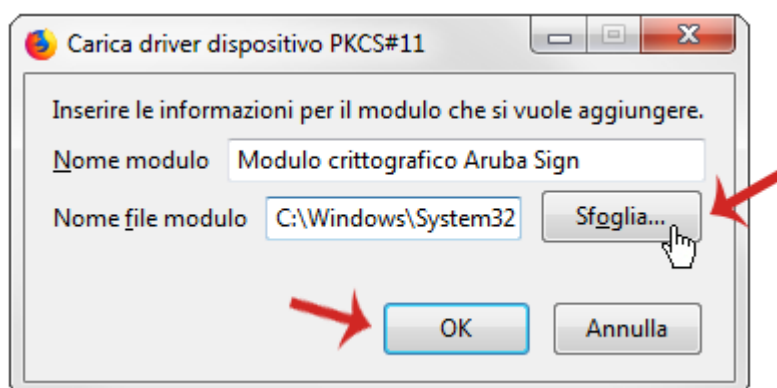
- 3) Da Privacy e sicurezza in alto a sinistra, scorrere fino a visualizzare Certificati in fondo alla pagina, quindi selezionare il tab Dispositivi di Sicurezza;
- 4) Dal Pannello **Gestione Dispositivi**, cliccare sul pulsante **Carica**:



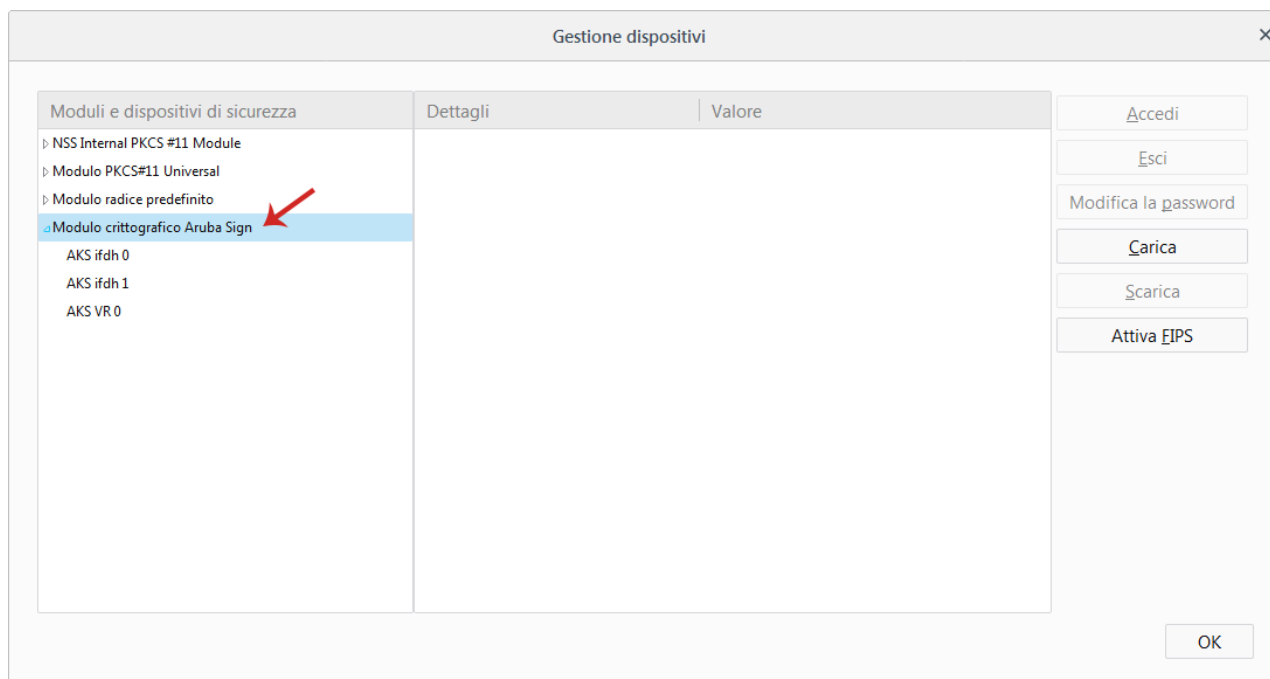
Al Tab "Carica dispositivo PKCS#11" visualizzato, procedere come di seguito indicato:

76

- Su "Nome modulo" indicare una stringa descrittiva che identifichi il modulo crittografico che si sta aggiungendo;
- Utilizzare **Sfogliare** per spostarsi all'interno della directory C:\WINDOWS\system32 e selezionare il file **bit4xpki.dll**;
- Una volta selezionato, verificare che il campo Nome file modulo sia valorizzato con il percorso della libreria;
- Cliccare su **Ok** per proseguire:



- 1) Verificare che all'interno della finestra **Gestione dispositivi** compaia il nuovo modulo appena aggiunto quindi cliccare su **OK**:



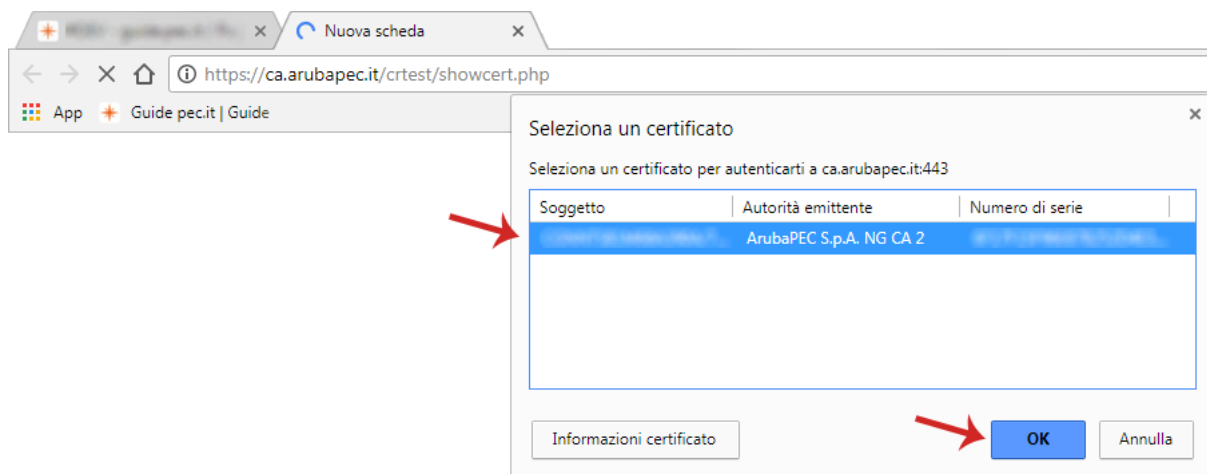
Terminata la procedura di import manuale dei certificati è terminata ed è **possibile effettuare l'accesso tramite il certificato CNS. Nel caso in cui i certificati di firma e CNS vengano importati all'interno dello Store di Mozilla FireFox** in alcun modo cliccare sul pulsante **Elimina**. L'azione potrebbe causare l'eliminazione dei certificati CNS e Firma digitale all'interno della Smart Card e l'impossibilità di recuperarli.

77

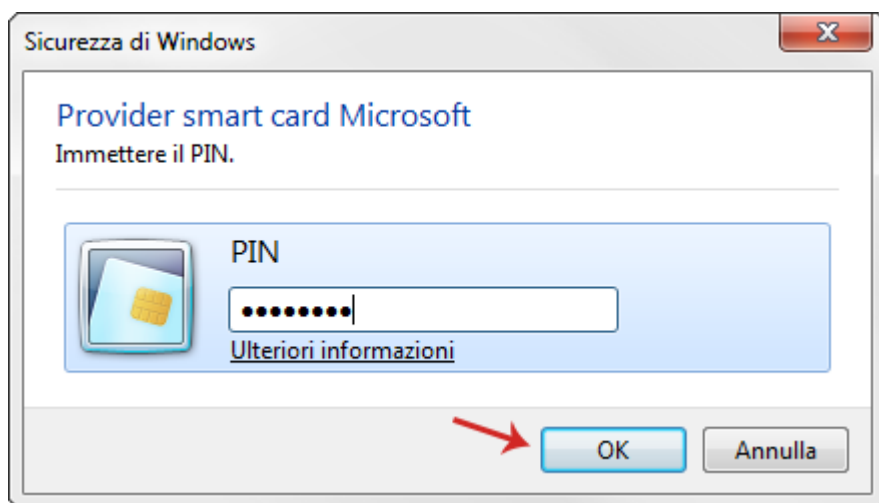
Verifica corretta importazione Certificato Aruba sign su Google Chrome

Questa procedura consente l'accesso a un sito di test con il proprio certificato CNS. Per procedere:

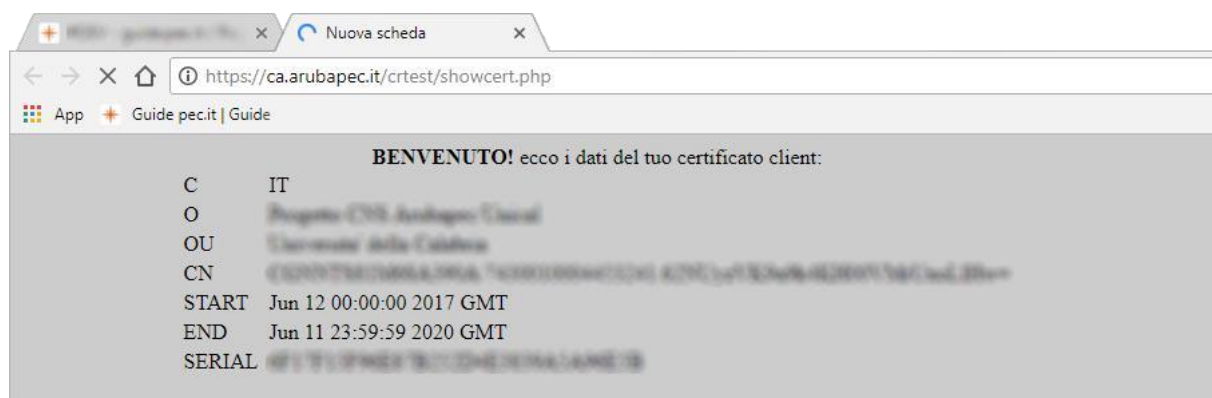
- 1) Avviare Google Chrome;
- 2) Collegarsi al link <https://ca.arubapec.it/crtest/showcert.php>;
- 3) Selezionare il certificato da utilizzare per l'accesso e cliccare su "Ok":



4) Inserire il PIN della Smart Card e cliccare su "**Ok**":



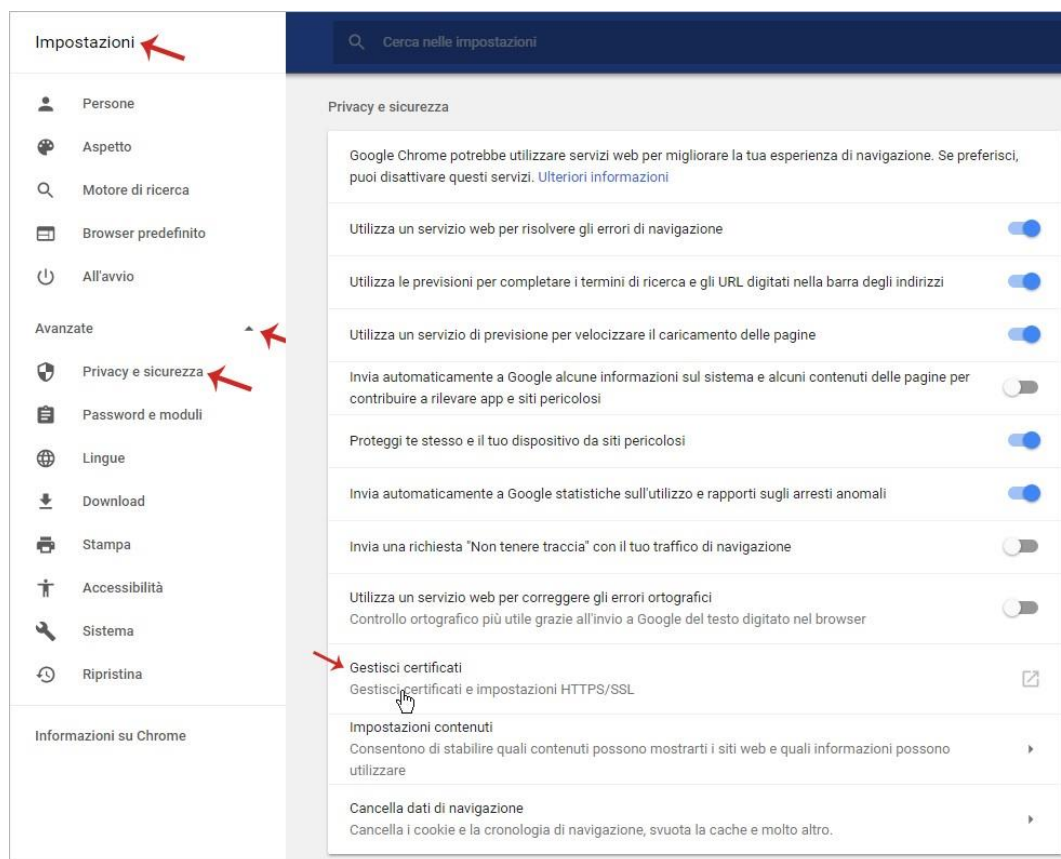
5) Verificare che il Browser mostri la pagina riepilogativa contenente i dati del certificato usato per l'accesso sicuro:



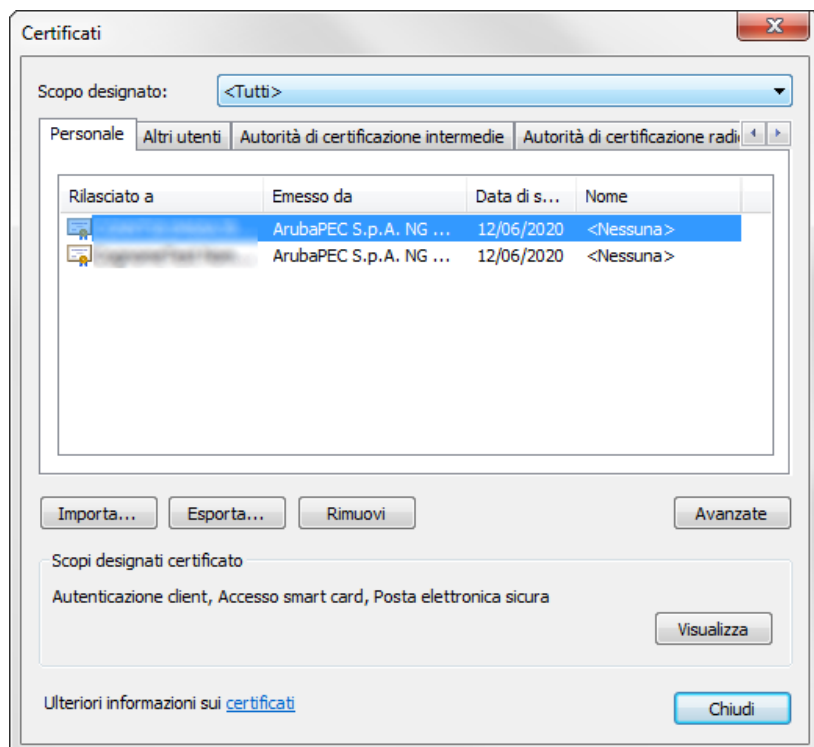
Verificare la corretta importazione del Certificato da "Strumenti" di Google Chrome:

Questa procedura consente di verificare l'effettivo caricamento dei Certificati, e quindi il corretto esito della procedura di **"Import Certificato"**. Per procedere:

- 1) Avviare Google Chrome;
- 2) Selezionare dal menù in alto a destra in alto a destra l'icona "Opzioni";
- 3) Dal menù in alto a destra "Impostazioni" selezionare "Avanzate > Privacy e Sicurezza > Gestisci Certificati":



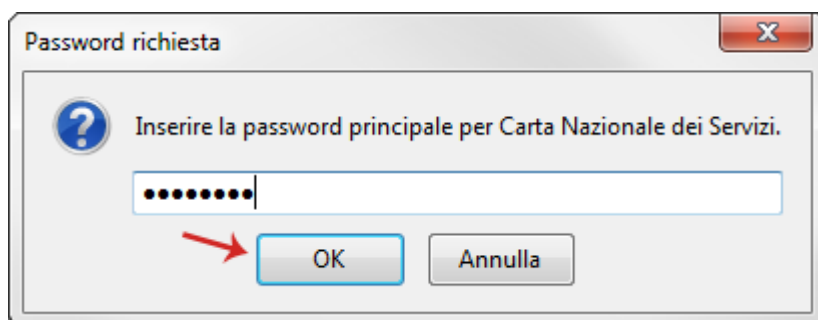
Col kit di Firma Digitale collegato al PC, deve comparire in elenco il Codice Fiscale relativo al proprio Certificato:



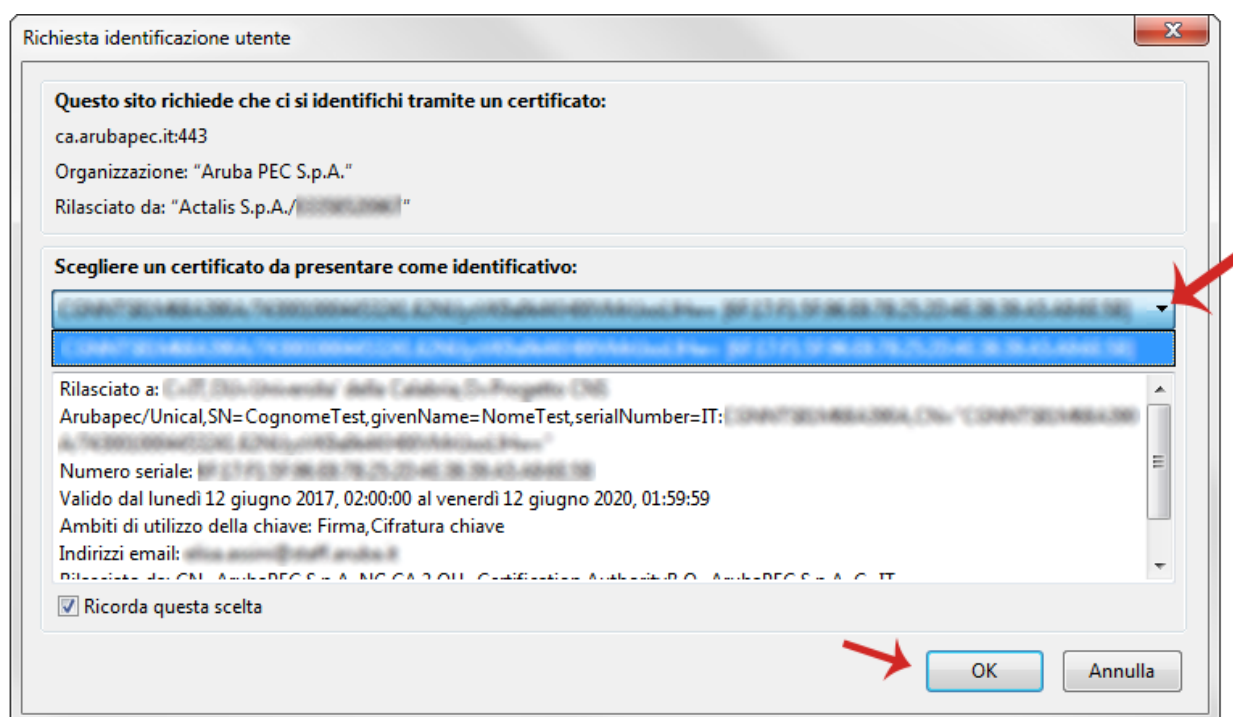
Verifica corretta importazione Certificato Aruba Sign su Mozilla Firefox

Questa procedura consente l'accesso a un sito di test con il proprio certificato CNS. Per procedere:

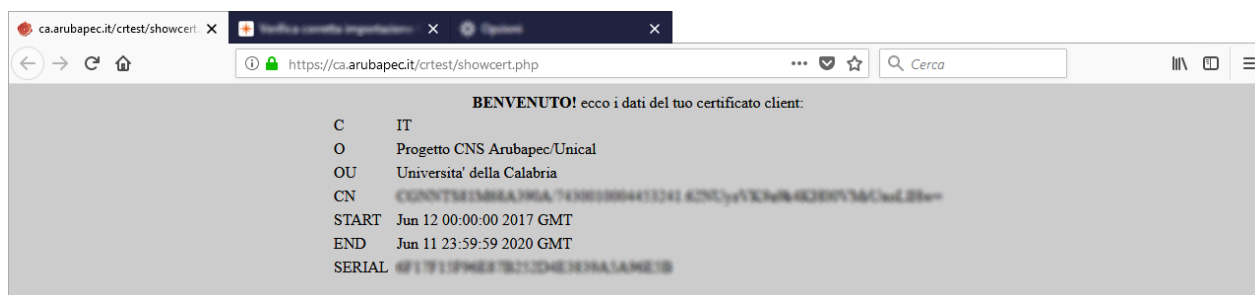
- 1) Avviare Mozilla Firefox;
- 2) Collegarsi al link <https://ca.arubapec.it/crtest/showcert.php>;
- 3) Inserire il PIN della carta e spuntare su "Ok":



Alla finestra "Richiesta Identificazione Utente" selezionare il certificato da utilizzare per l'accesso e cliccare su "Ok":



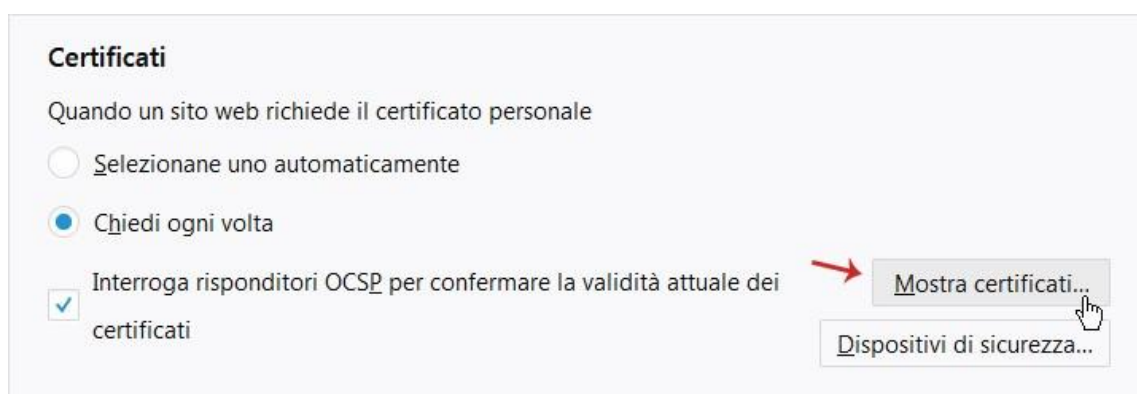
- 1) Verificare che il Browser mostri la pagina riepilogativa contenente i dati del certificato usato per l'accesso sicuro:



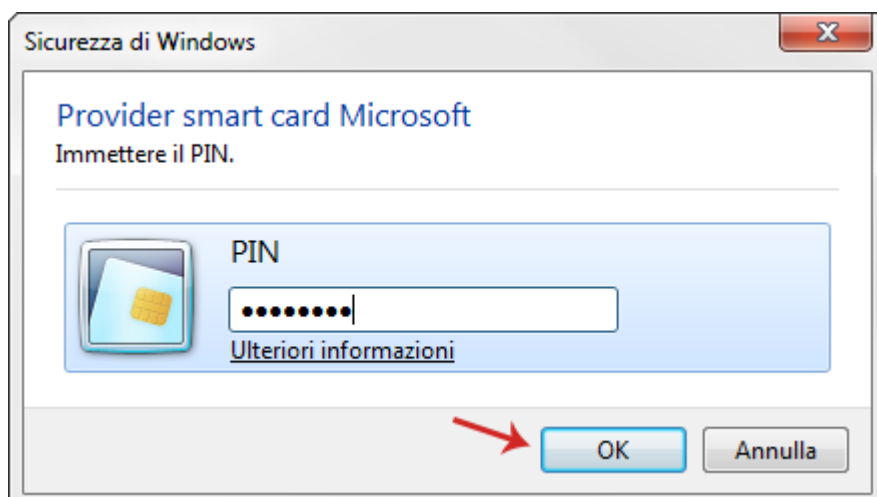
Verificare la corretta importazione del Certificato da "Strumenti" di Mozilla Firefox:

Questa procedura consente di verificare l'effettivo caricamento dei Certificati, e quindi il corretto esito della procedura di **"Import Certificato"**. Per procedere:

- 1) Avviare Mozilla Firefox;
- 2) Dall'icona "Strumenti" in alto a destra, scegliere "Opzioni";
- 3) Da "Privacy e sicurezza" in alto a sinistra, scorrere fino a visualizzare "Certificati" in fondo alla pagina, quindi selezionare il tab "Mostra Certificati":

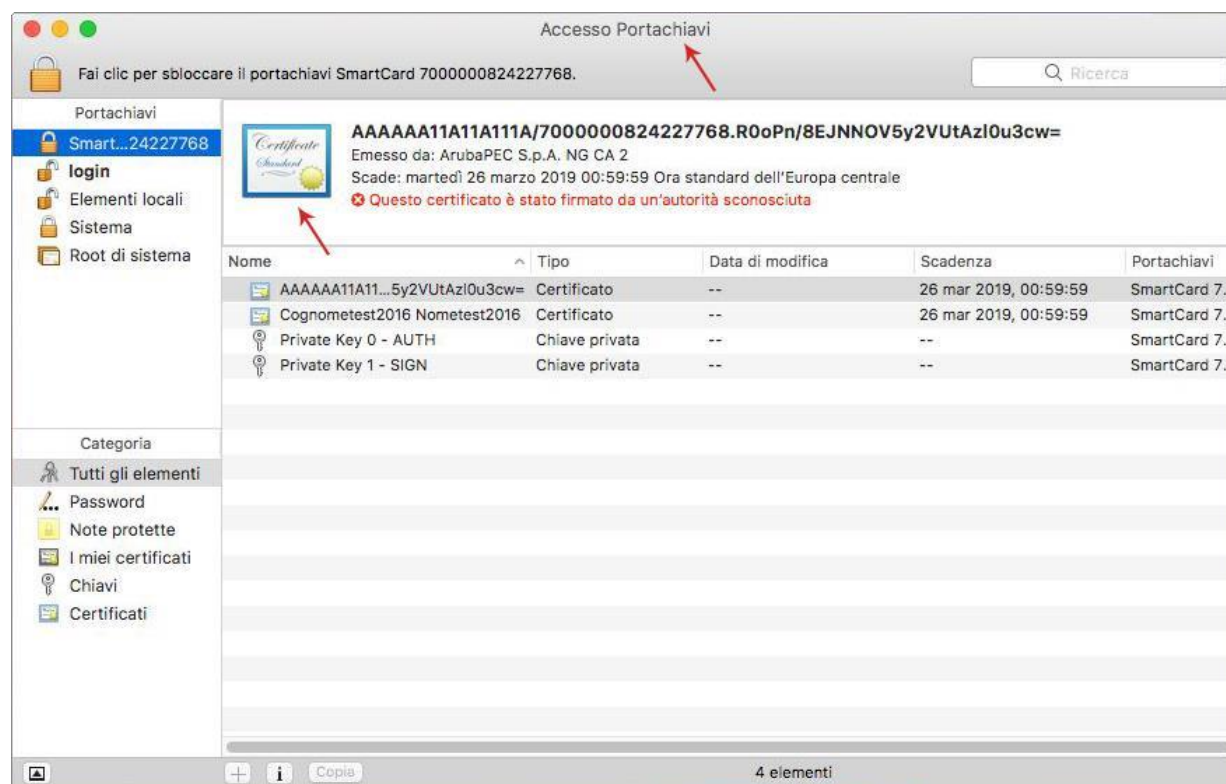


- 1) Inserire il PIN della Smart Card e cliccare su "Ok":



Import Certificato" con Aruba Sign (MAC)

La funzione **"Import Certificato"** su MAC per **Aruba Sign** è **automatica**. Una volta installato il Software, i certificati sono importati nel **"Portachiavi"** del MAC. Il certificato è visualizzato come da immagine esemplificativa sottostante:

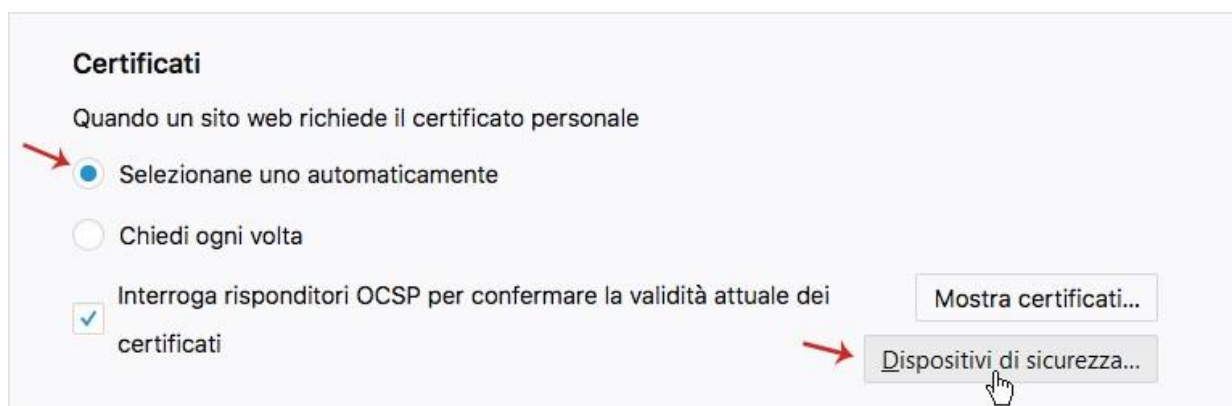


82

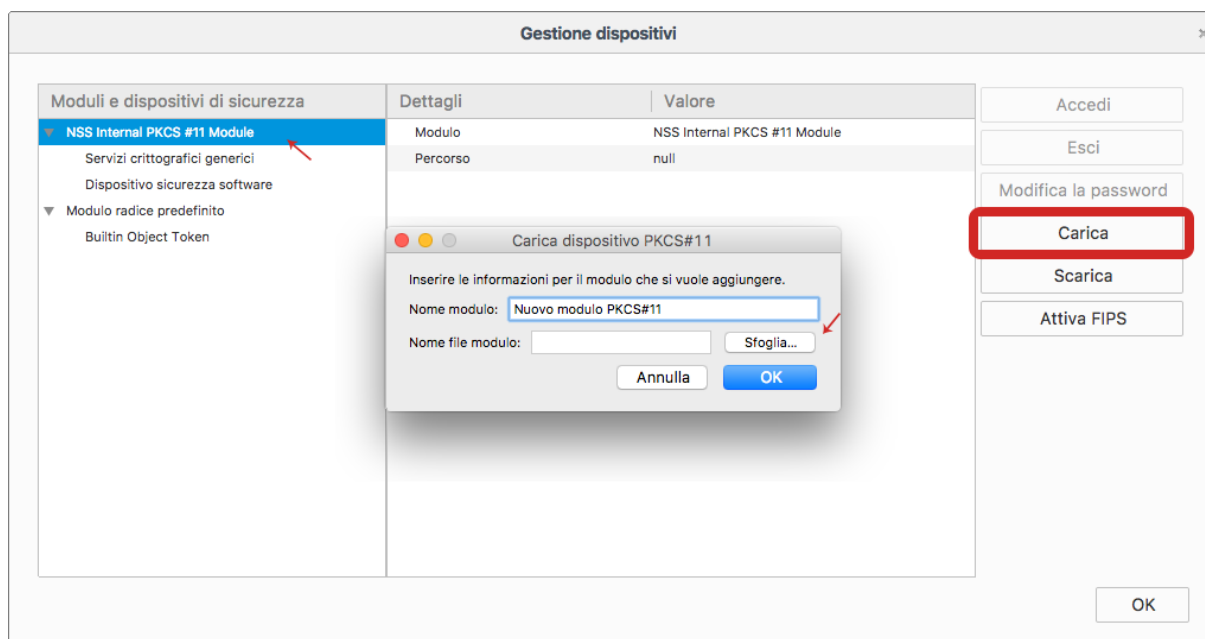
Dalla versione 10.6 alla 10.9 di MAC per poter utilizzare Safari per autenticazioni tramite Smart Card, si rimanda alle guide specifiche del produttore (il Certificato deve essere scaricato con codice fiscale in formato .cer tramite Aruba Sign).

In alternativa è possibile utilizzare Mozilla Firefox per autenticazioni tramite Smart Card. Per procedere:

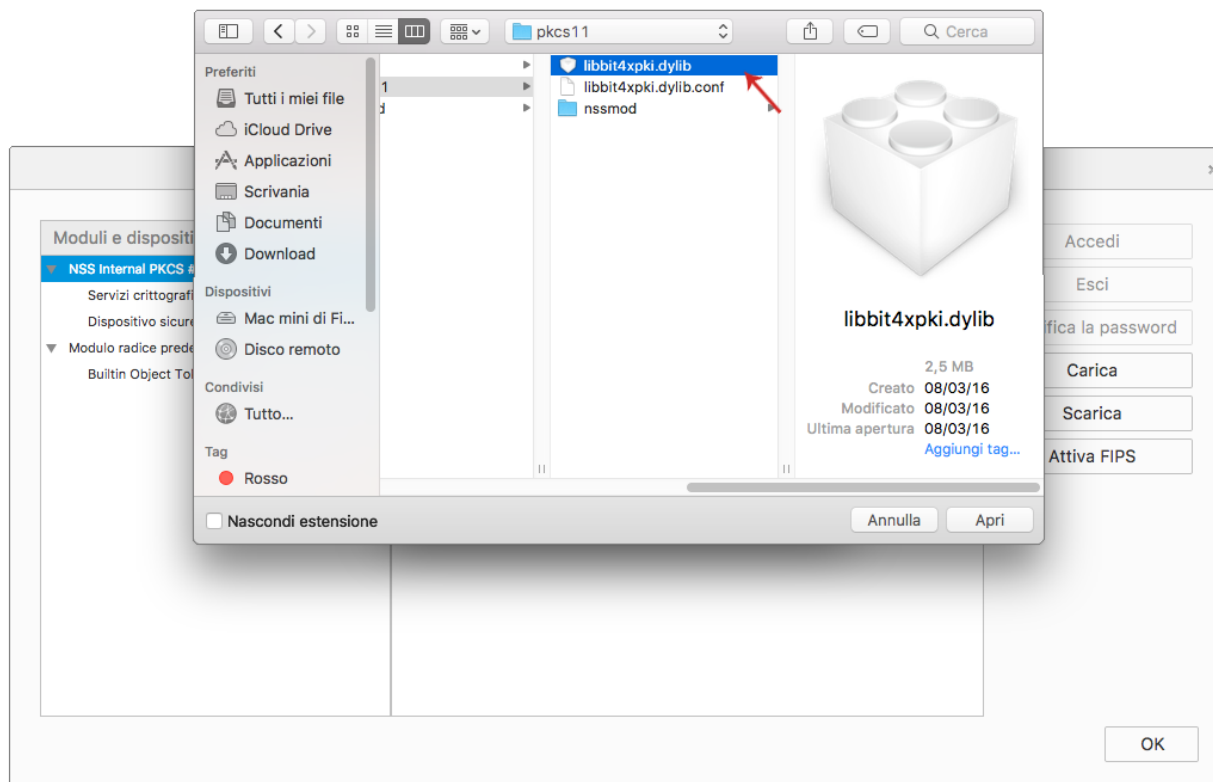
- 1) Avviare Mozilla Firefox;
- 2) Dall'icona "Strumenti" in alto a destra, scegliere "Preferenze";
- 3) Da "Privacy e sicurezza" in alto a sinistra, scorrere fino a visualizzare "Certificati" in fondo alla pagina;
- 4) Spuntare l'opzione "Selezionane uno automaticamente" quindi "Dispositivi di Sicurezza":



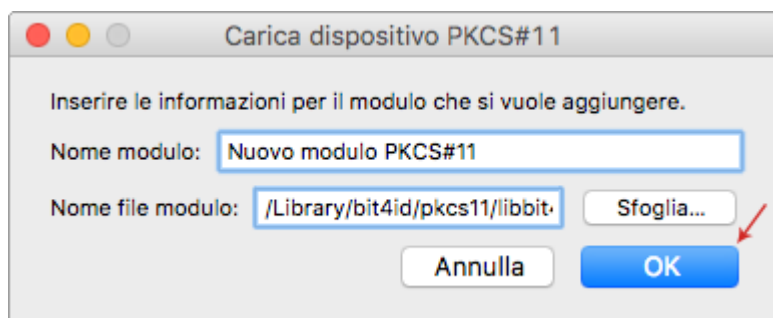
- 1) Nella finestra "**Gestione dispositivi**" selezionare a sinistra "**NSS Internal PKCS # 11 Module**" quindi cliccare sul pulsante "**Carica**":



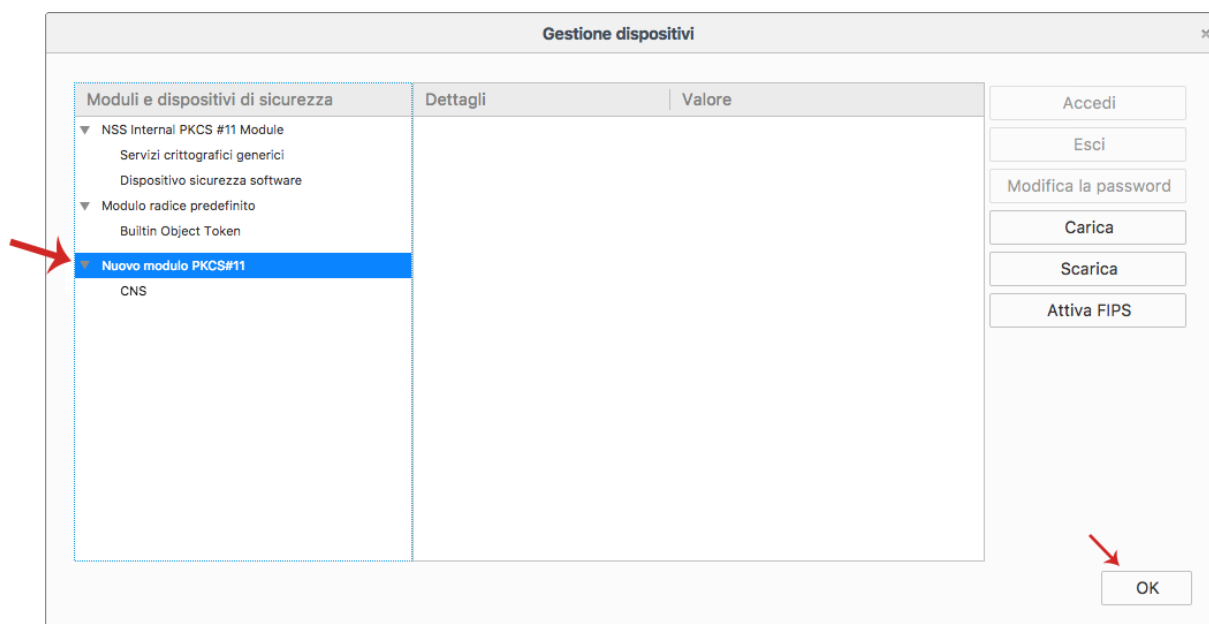
- 1) Al Tab "**Carica dispositivo PKCS#11**" visualizzato utilizzare "**Sfoglia**" per spostarsi all'interno della directory e selezionare il file **libbit4xpki.dylib**:



- 1) Verificare che il campo Nome file modulo sia valorizzato con il percorso della libreria selezionata utilizzando il tasto **"Sfoglia"** come indicato allo Step precedente e cliccare su **"Ok"** per proseguire:



- 1) Verificare che all'interno della finestra **"Gestioni dispositivi"** compaia il nuovo modulo appena aggiunto quindi cliccare su **"Ok"**:



Mozilla Firefox è pronto per essere utilizzato per autenticazioni tramite Smart Card.

Nel caso in cui i certificati di firma e CNS vengano importati all'interno dello Store di Mozilla FireFox in alcun modo cliccare sul pulsante **"Elimina"**. L'azione potrebbe causare l'eliminazione dei certificati CNS e Firma digitale all'interno della Smart Card e l'impossibilità di recuperarli.